Accepted for publication in *European Journal of Consumer Law/ Revue européenne de droit de la consummation* published by Larcier

THE INTERNET OF THINGS AT THE INTERSECTION OF DATA PROTECTION AND TRADE SECRETS. NON-CONVENTIONAL PATHS TO COUNTER DATA APPROPRIATION AND EMPOWER CONSUMERS

Guido Noto La Diega – Cristiana Sappa*

Abstract

The Internet of Things (IoT) has heralded a never-before-seen quantity of high-quality data. This includes both personal and non-personal data. Factual and legal control over IoT data gives companies unparalleled power to influence consumers, policy makers, and the other stakeholders of the IoT's supply chain. The combination of analytics algorithms, the data goldmine structure and the output of data processes are regularly kept secret by businesses. Leveraging this portfolio of big data and trade secrets, IoT companies put in place practices that can negatively affect consumers, who are often unaware of them due to technical and legal secrecy. 'Technical' secrecy results from the opacity of the algorithms that underpin the IoT, especially when AI-enabled. 'Legal' secrecy, in turn, come from a combination of trade secrets and strategic contract management that keep IoT data practices secret. This begs the central research question of this article: how can consumers be empowered to counter IoT data appropriation?

Traditional consumer protection approaches, epitomised by the Consumer Rights Directive, are focused on pre-contractual duties to inform consumers. Their benefit to IoT consumers is limited by their reflecting a text-based paradigm, whereby information must be legible. This is not fit for the IoT, where displays tend to disappear and information is provided in audio or video formats. Consumer laws are drafted on the assumption of information asymmetries in business-to-consumer contracts, but they fail to account for the power imbalances that permeate IoT transactions. These power imbalances are exacerbated by control over a wealth of user data and corresponding granular knowledge of consumers' vulnerabilities, behaviors, and biases. This knowledge can be used to impose opaque practices on consumers; among these, IoT data appropriation by means of trade secrets plays a key role.

* Guido Noto La Diega is Associate Professor of Intellectual Property and Privacy Law at the University of Stirling; Chair of SCOTLIN (Scottish Law and Innovation Network); Fellow of the Nexa Center for Internet and Society; Visiting Professor at the Università degli Studi di Macerata; Researcher at CRISP (Centre for Research into Information, Surveillance & Privacy). Cristiana Sappa is Associate Professor of Business Law at Iéseg School of Management, Research Fellow at Centre d'Etudes sur le Droit de l'Immatériel (CERDI). This work is the output of a joint effort, however while both authors drafted Section I, Cristiana Sappa mainly drafted Section III, and Guido Noto La Diega mainly drafted Section II, IV, and V. We wish to thank Professor Tanya Aplin and the anonymous peer-reviewers for the helpful comments on a previous draft. The preliminary findings of this research have been presented at the *1st Future of Law Conference: The Internet of Things, smart contracts, and intelligent machines* (Singapore Management University School of Law, Singapore, 27 October 2017), at *Gikii* (Wien Universität, Vienna, 14 September 2018), and at the *111th Annual Conference of the Society of Legal Scholars* (University of Exeter, 1 September 2020). We are thankful to the participants for the useful feedback and the encouragement. We are also grateful to James C. Bell for the kind proofreading. The responsibility for the views expressed in this paper, and for any errors herein, rests with us.

Therefore, an emergent concern is whether the law provides tools that effectively safeguard consumers' interests, in particular by ensuring substantial transparency as to the actual use of their personal data. How can this can be guaranteed, and the consumer empowered in a post-interface world of profoundly imbalanced relationships? The answer cannot be found solely within the trade secrets' regime: data protection needs to be considered.

This article focuses on the trade secrets exceptions of legitimate interest and freedom of information, and on the General Data Protection Regulation (GDPR)'s rights to access, data portability, information, and not to be subject to solely automated decisions. We put forward that trade secrets' exceptions and GDPR rights re-balance the interests of consumers vis-à-vis big IoT players such as Amazon. Specifically, they can positively contribute to transparency, consumers autonomy, information symmetry, data portability, and freedom of choice. We propose a holistic approach that empowers consumers by countering data appropriation, thus redistributing data control.

I. Introduction: scope of the research and methods

The Internet of Things (IoT) has heralded a never-before-seen quantity of high-quality data, including personal data. Factual and legal control over IoT data gives companies unparalleled power to influence consumers, policy makers, and the other stakeholders of the IoT's supply chain. The combination of analytics algorithms, the data goldmine structure and the output of data processes are regularly kept secret by businesses.[1] Leveraging this portfolio of big data and trade secrets, IoT companies put in place practices that can negatively affect consumers, who are often unaware of them due to a technical and legal secrecy. 'Technical' secrecy results from the opacity of the algorithms that underpin the IoT, especially when AI-enabled. 'Legal' secrecy, in turn, comes from a combination of trade secrets and strategic contract management that keep IoT data practices secret. Thanks to the data power[2] that IoT big players such as Amazon and Google hold, they can take advantage of their dominant position to impose contracts that try and justify unfair and opaque practices, including the appropriation and re-use of personal as well as non-personal data (hereinafter 'data appropriation')[3].

---

[1] See M. M. MAGGIOLINO, "EU Trade Secrets and Algorithmic Transparency", *AIDA 2019*, forthcoming, stating that the EU Directive on trade secrets does not directly impose any form of algorithmic transparency. And links this to the fact that it was born with the specific aim of sheltering secrets from misappropriation, espionage, theft or any other species of unfair behavior. Thus, one cannot expect the Directive to explicitly regulate the cases in which secrets must be disclosed and algorithms must be made transparent. Nevertheless, the Directive recognizes the existence of cases in which the above-described commercial interests can give way to the protection of other values.

[2] O. LYNSKEY, "Grappling with 'Data Power': Normative Nudges from Data Protection and Privacy", *Theoretical Inquiries in Law*, 2019/1, p. 189.

[3] It is a common misunderstanding that IoT data escapes data protection laws because it qualifies as 'machine data' and, therefore, it would count as non-personal data. D. SUPRIYADI, *Personal and Non-Personal Data in the Context of Big Data*, Tilburg, Tilburg Institute for Law, Technology and Society, 2017, p. 30. This misunderstanding is based on a twofold incorrect assumption. First, it assumes that all IoT data is machine data. On the contrary, especially in the context of consumer IoT (e.g. smart home), the Thing can send back

As evidence of the fact that data appropriation practices are mostly kept private, one can consider Amazon's Alexa as a case study. Amazon does not tell consumers which data they collect about them. They only disclose "the types of information we gather"[4]. They merely provide "examples of information collected"[5]. This includes data that consumers provide (e.g. account information), automatic information (e.g. cookies), and data from unspecified "other sources" (e.g. when consumers authorise a third-party website, such as Facebook, to interact with the Thing). Amazon does not disclose for which purposes data are collected and processed, they only list examples of such purposes, which include advertising and unspecified "purposes for which we seek your consent".[6] Additionally, Amazon shares consumers' personal data with Amazon.com, Inc.,'s subsidiaries. Most of them are established in the US but only 5 of them are Privacy-Shield-certified, which means that it is unclear whether the transfers of EU residents' personal data to the US has a legal basis. This is all the more true after the recent *Schrems III*[7] ruling that invalidated the Privacy Shield leaving companies with no clear legal basis for international data transfers. Finally, as discovered through a subject access request we submitted in March 2019, Amazon grants consumers access only to some of their personal data, mainly the data that the consumer provided and the times when the consumer interacted with Amazon's Things and services. This data is provided without any explanation and in a format that is hard to decipher, as seen in Table 1 below. These data, if taken in isolation, may appear to be non-personal, but if combined with data from others sources (e.g. other Things) can easily become personal.

Table 1. Extract from Amazon's reply to one of the co-authors' subject access request.

Device	**Data source name**[8]	**Country of**	**Software version**

to manufacturers not only data about the Thing itself (e.g. when a movement sensor is activated) but also granular data about the consumer's behavior. Second, even machine data can count as personal data. Aggregating and re-combining data from multiple Things and other sources, data that, considered individually, would be non-personal, can become personal See e.g. R. ALLSOPP, "Levelling the odds? Big data analytics in the online gambling industry and the application of the GDPR" in M. M. CARVALHO, *Law & Technology*. *E.Tec Yearbook*, Minho, University of Minho, 2018, p. 135.

[4] Amazon's Privacy Notice, last updated on 22 March 2019 <https://www.amazon.co.uk/gp/help/customer/display.html/ref=hp_left_v4_sib?ie=UTF8&nodeId=201909011> accessed 1 May 2019.

[5] Ibidem.

[6] Ibidem.

[7] Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* (CJEU, 16 July 2020).

[8] In the spreadsheet that was sent as a reply to our subject access request, Amazon uses the obscure acronym 'DSN' that interpret as referring to an equally obscure concept, that is 'data source name'. This is defined as a "means of identifying, and connecting to, a database (…) required for many Web applications that interact with and query databases" (F. BOTTO, *Dictionary of e-Business*, Chichester, Wiley, 2nd ed., 2003, p. 109). This would suggest that Amazon has a database that includes all users' personal data, which begs the question of whether the sui generis right could be used to appropriate said data. See more on this in C. SAPPA, "How Data Protection Fits with the Algorithmic Society via Two Intellectual Property Rights – A Comparative Analysis", *GRUR Int*., 2019, p. 135; and *JIPLP*, 2020, p. 407; G. NOTO LA DIEGA, "Artificial Intelligence and Databases in the Age of Big Machine Data", *AIDA 2018*, 2019, p. 93.

record time		**residence**	
21/03/2019 01:24	G070L8118454139U	GB	288.6.3.2_user_632552020
21/03/2019 01:24	G070L8118454139U	GB	288.6.3.2_user_632552020
21/03/2019 00:28	G090RF04743204M2	GB	288.6.3.1_user_631550720
21/03/2019 00:28	G090RF04743204M2	GB	288.6.3.1_user_631550720
20/03/2019 20:50	G070L8118454139U	GB	288.6.3.2_user_632552020
20/03/2019 20:25	G090RF04743204M2	GB	288.6.3.1_user_631550720
19/03/2019 20:04	G070L8118454139U	IT	288.6.3.2_user_632552020

It does not include, for example, the profile that Amazon builds about their users based on their personal data; it excludes those precious inferences that are increasingly recognised as personal data.[9] For example, Amazon stores the recording of the user's interactions with Alexa.[10] Thanks to its emotion recognition technologies, Amazon can extract from users' voice valuable information about their feelings, information that can be utilized to target them more effectively. Once interrogated to obtain more information about our data – beyond the obscure spreadsheets with which the company thought to comply with our subject access request – Amazon did not comply with our requests. One may conjecture that this is because Amazon subjects the rights to access, correct, port, and delete to the "applicable law" and the applicable law also protects information covered by trade secrets.

Traditional consumer protection approaches are not, in themselves, sufficient to tackle consumers' issues in the IoT.[11] Three cornerstones of consumer protection are the

[9] S. WACHTER, B. MITTELSTADT, "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI", *Columbia Business Law Review*, 2019/2, p. 494.

[10] Amazon's Privacy Policy.

[11] Future research should explore if the most recent consumer laws are more suitable to tackle IoT data appropriation. One such law in the Enforcement and Modernisation of Consumer Protection Directive (Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules, O.J. L 328, 18.12.2019, p. 7). This Directive, effective as of 7 January 2020, has amongst other things amended the Consumer Rights Directive (Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, O.J. L 304, 22.11.2011, p. 64). For

pre-contractual duties to inform, the non-binding nature of unfair terms, and outlawing of unfair commercial practices. First, the Consumer Rights Directive,[12] in imposing an obligation to inform consumers in a legible way clearly reflects a text-based paradigm that is not fit for an IoT world where video-user and audio-user interfaces prevail and often the lack or limited size of displays prevent the information from being communicated as text.[13] Audio- or video-communication may be more effective but could not comply with the requirement of legibility.[14] Second, from the Unfair Terms Directive[15] stems the non-binding nature of unfair terms and thus it aims to address the "significant imbalance in the parties' rights and obligations arising under the contract"[16]. This Directive has not been drafted taking account of the power imbalance that is exacerbated by the control over a wealth of user data; and corresponding granular knowledge of consumers' vulnerabilities, behaviors, and biases. This knowledge - and imbalance - can be used to impose on consumer practices that are rarely written in contracts, as they are kept secret. [17] For example, nowhere in Facebook's terms and conditions could be found disclosure of the company's emotional manipulation experiments.[18] A traditional consumer regime that goes beyond the contract, and that therefore, in principle, may be of more help, is the Unfair Commercial Practices Directive.[19] However, this regime focuses on a consumer who is about to conclude a transaction and looks at the unfairness of a practice's economic consequences and therefore is not fit for the more subtle practices that IoT data allows company to put in place, which may not be linked to a transaction.[20]

An emergent concern is whether the law provides tools that effectively safeguard consumers' interests, in particular by ensuring substantial transparency as to the actual use of IoT-generated personal data. The question is how this can be guaranteed, in a way that takes into account that we live in a profoundly imbalanced post-interface world, where

---

instance the latter now provides that, whilst in respect of personal data traders must comply with the GDPR, they can use content provided or created by consumers when using digital content or services in a number of scenarios, including when the content "has been aggregated with other data by the trader and cannot be disaggregated or only with disproportionate efforts" (art 13(5)(c)). This could encourage an analysis on what can be appropriated and which legal device would be the most suitable.

[12] Arts 7(1), 8(1), 8(2), 8(3), and recital 38.

[13] C. BUSCH, "Does the Amazon Dash Button Violate EU Consumer Law? Balancing Consumer Protection and Technological Innovation in the Internet of Things", *EuCML* 2018, 78.

[14] On the consumer issues in an interface-free world see E. MIK, "The Disappearing Computer: Consent in the World of Smart Objects" *This Journal*, 2020.

[15] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, O.J. L 95, 21.4.1993, p. 29.

[16] Unfair Terms Directive, art 3(1).

[17] G. NOTO LA DIEGA, *Internet of Things and the Law*, Abingdon-on-Thames, Routledge, 2020.

[18] C. FLICK, "Informed consent and the Facebook emotional manipulation study" *Research Ethics*, 2016, 12(1), p. 14.

[19] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council, O.J. L 149 11.6.2005, p. 22.

[20] N. HELBERGER, "Profiling and Targeting Consumers in the Internet of Things–A New Challenge for Consumer Law" in R. SCHULZE, D. STAUDENMAYER (eds), *Digital Revolution: challenges for contract law in practice*, Baden-Baden, Nomos, 2016, p. 135.

information is communicated in unconventional ways, the imbalance is not formalized in contracts, and it takes subtle forms that may not be captured in a formal contractual document.

A first answer could rely on private ordering initiatives, such as open licensing,[21] but being the outcome of a voluntary commitment they are insufficient to tackle this ubiquitous issue. In turn, competition law can compensate the lack of legal security for consumers, but it operates ex post. We argue that consumers can be better protected by measures that intervene ex ante; the answer can be searched for in the way trade secrets and data protection regimes are structured. Trade secrets are protected by a set of legal rules that were introduced mainly to favor the market operators' interests. However, their scope of protection is not as wide as the one of other Intellectual Property Rights (IPRs) and they embed flexibilities, namely exceptions and limitations. In turn, the General Data Protection Regulation (GDPR)[22] protects consumers by means of more modern transparency requirements and other individual and collective rights that apply regardless of contracts and transactions. Some of its rights and obligations may be leveraged to counter IoT data appropriation. We argue that these regimes should be invoked in the context of a holistic strategy to better protect consumers.

We will show that trade secrets can cover IoT data, including personal data and algorithms. The conflict that ensues needs to be governed. This article focuses on the trade secrets exceptions of legitimate interest and freedom of information, and on the GDPR's rights to access, data portability, information, and not to be subject to solely automated decisions. We put forward that trade secrets' exceptions and GDPR rights re-balance the interests of consumers vis-à-vis big IoT players such as Amazon. Such a holistic approach empowers consumers by countering data appropriation, thus redistributing data control.

In terms of methods, this article explores the issue from an EU perspective, having in mind the relevant implementations of the selected regimes in the UK, Italy, and France.[23] Additionally, we have conducted text analysis of Amazon's privacy policy and explored its data practices by means of a data subject request, as well as interactions with its customer advisors.[24] More precisely Section II analyses data protection, Section III studies trade secrets laws. Then, Section IV examines interactions between these two sets of rules (Section IV).

II. Data protection issues in the Internet of Things

[21] See, albeit in passing, N. ZINGALES, "Of Coffee Pods, Videogames, and Missed Interoperability: Reflections for EU Governance of the Internet of Things", *TILEC Discussion Paper*, 2015-026, p. 1

[22] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR), O.J. L 119, 4.5.2016, p. 1.

[23] These are the countries where the authors are based.

[24] On the benefits of subject access requests as a research method in legal studies see R. L. P. MAHIEU, H. ASGHARI, M. VAN EETEN, "Collectively exercising the right of access: individual effort, societal effect" *Internet Policy Review*, 2018/3, p. 1. On qualitative research and text analysis see M. C. LACITY & M. A. JANSON, "Understanding Qualitative Data: A Framework of Text Analysis Methods" *Journal of Management Information Systems*, 1994/2, p. 137.

Effective as of May 2018, the GDPR replaced the Data Protection Directive[25] and increased the protection of personal data throughout the EU. It applies to personal data processed by entities that are either established in the EU or target EU residents.[26] Although being a regulation it is directly applicable in all Member States,[27] the latter have adopted implementing measures to regulate those aspects where countries have been left some discretion.[28] As to the jurisdictions we selected, Italy and France amended their existing data protection statutes, respectively the *Codice della Privacy*[29] and the *Loi informatique et libertés*.[30] Conversely, the UK repealed the relevant statute[31] and replaced it with the Data Protection Act 2018 that incorporates and supplements the GDPR.[32] The UK incorporation is of particular importance in light of the fact that the country left the EU on 31 January 2020 (so-called Brexit) and the retention of the same rules should guarantee the continuity of EU-UK data flows. There are strong incentives to maintain convergence, since "EU personal data-enabled services exports to the UK were worth approximately £42bn (€47bn) in 2018, and exports from the UK to the EU were worth £85bn (€96bn)"[33]. Accordingly, the UK government is seeking an adequacy decision, i.e. the European Commission's confirmation that a non-EEA country provides an adequate level of personal data protection.[34]

The GDPR is not about secrecy. This may seem counterintuitive. Indeed, pseudonymisation is one of the recommended measures[35] and companies tend to anonymise data in the hope that this will bring the processing outside of the scope of the

[25] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive), O.J. L 281, 23.11.1995, p. 31.
[26] GDPR, art 3.
[27] Treaty on the Functioning of the European Union (TFEU), O.J. C 115, 9.5.2008, p. 171, art 288. On the limited role of Member States when a regulation is passed see Judgement of 31 January 1978, 94/77, Fratelli Zerbone Snc v Amministrazione delle finanze dello Stato, EU:C:1978:17.
[28] Cf. D. AMRAM, "Building up the 'Accountable Ulysses' model. The impact of GDPR and national implementations, ethics, and health-data research: Comparative remarks", *Computer Law & Security Review*, 2020/37, p. 1.
[29] *Decreto legislativo* 20 June 2003 n° 196 "*Codice in materia di protezione dei dati personali*", as amended by the *decreto legislativo* 10 August 2018 n° 101. See G. FINOCCHIARO. "Italy: The Legislative Procedure for National Harmonisation with the GDPR", *Eur. Data Prot. L. Rev.*, 2018/4, p. 496.
[30] *Loi* n° 78-17 of 6 January 1978 *relative à l'informatique, aux fichiers et aux libertés*, as amended by the *Loi* n° 2018-493 of 20 June 2018 *relative à la protection des données personnelles*. See F. VINEY, "La loi relative à la protection des données personnelles", in *Actualité juridique. Famille*, 2018, p .366.
[31] Data Protection Act 1998.
[32] Data Protection Act 2018, s 4; European Union (Withdrawal) Act 2018, s 3.
[33] Department for Digital, Culture, Media & Sport, "Explanatory Framework for Adequacy Discussions – Section A: Covering Note" (*UK Gov*, 13 March 2020) 1 <https://www.gov.uk/government/publications/explanatory-framework-for-adequacy-discussions> accessed pm 1 May 2020.
[34] GDPR, art 15; Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA ('Law Enforcement Directive), O.J. L 119, 4.5.2016, p. 89, art 36.
[35] GDPR, art 6(4)(e).

GDPR.[36] Such a strategy is based on the fact that principles of data protection should not apply to anonymous information. Yet, it does not consider that anonymization alleviates companies of the burden of GDPR compliance only when the data subject is no longer identifiable.[37] The IoT, however, enables re-identification, as noted in section [IV] herein after.

The misunderstanding of the GDPR as a privacy – and even secrecy – law has led to risks for consumers. The reliance on anonymisation and other forms of confidentiality-focused privacy-enhancing technologies is leaving data "re-identifiable by capable adversaries while heavily limiting controllers' ability to provide data subject rights, such as access, erasure and objection, to manage this risk "[38]. The point is that the GDPR espouses a concept of data protection that focuses on control, rather than privacy as confidentiality.[39] Data control is exercised through rights such as access, rectification, and portability. This is consistent with the GDPR's goal to facilitate the free flow of personal data within the Union[40] and eliminate the differences between national laws that are regarded as an obstacle to the pursuit of economic activities at the level of the Union and distort competition.[41] In this sense, we argue that the GDPR is underpinned by a philosophy of openness and control, rather than secrecy and privacy.

As an analytical framework to shed light on the main data protection issues in the IoT, this section will refer to the Article 29 Working Party's opinion on the IoT.[42] The framework needs adapting. Indeed, the opinion considered the data protection issues in the IoT with reference to the Data Protection Directive. However, the GDPR can be mostly regarded as the codification of best practices that developed under the Data Protection Directive;[43] therefore, most of the considerations that the Article 29 Working Party made retain their validity. The framework has also been adapted to take account of phenomena on which only recently the scholarly debate has started developing, namely inferences and digital dispossession.

The main data protection issues in the IoT are:

(i) Lack of control and information asymmetry;
(ii) Quality of consent;
(iii) Inferential data and repurposing;
(iv) Anonymisation's limits;

[36] M. VEALE - R. BINNS - J. AUSLOOS, 'When data protection by design and data subject rights clash', *IDPL* 2018, p. 105.
[37] GDPR, recital 26.
[38] M. VEALE, R. BINNS, J. AUSLOOS, *op. loc. cit.*
[39] ARTICLE 29 WORKING PARTY, WORKING PARTY ON POLICE AND JUSTICE, 'The Future of Privacy: Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data", 2009/WP 168, p. 1; S. GÜRSES, "Can You Engineer Privacy?", *Communications of the ACM*, 2014/57, p. 20. The Article 29 Working Party, pan-European advisory group in matters of data protection, has been replaced by the European Data Protection Board on 25 May 2018.
[40] GDPR, recitals 6 and 9.
[41] GDPR, recital 9.
[42] ARTICLE 29 WORKING PARTY, "Opinion 8/2014 on the Recent Developments on the Internet of Things" *WP 223*, 2014.
[43] See e.g. P. DE HERT, V. PAPAKONSTANTINOU, "The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals" *Computer Law & Security Review*, 2012, 28, p. 130.

(v) Data appropriation.

First, there are connected issues of lack of control[44] and information asymmetry.[45] The difficulty to control how Things interact and to know which data the Thing sends back to the manufacturer makes it difficult to assert data control, especially because IoT companies keep these practices secret. Similar issues arise with big data and cloud computing, but as noted by the Article 29 Working Party the possibility to combine data from multiple sources exacerbates the loss of control.[46] This is perhaps best illustrated by IoT-enabled third-party monitoring, which may lead to the user losing control over how their data is processed. IoT systems are characterised by a high level of automation. Thing-to-Thing communication can take place automatically, without any citizen awareness. As an example of lack of control in the IoT, digital advertising company Improve Digital point out in their privacy policy that their clients sell advertising space on Things, and that 'for most of such devices it is *not possible to generally not allow cookies or opt-out*, although you can often remove all cookies.'[47] Whilst direct marketing can act as a legitimate interest under the GDPR[48] – and therefore controllers would not need to seek the data subject's consent when processing data for direct marketing purposes – the use of cookies or similar identifiers require consent under the e-Privacy Directive.[49] Moreover, even though the legitimate interests of third parties may justify third-party monitoring, IoT users have a right to object to that processing of their personal data. In principle, this is not an absolute right because data controllers could demonstrate compelling, overriding, and legitimate grounds for the processing.[50] However, IoT users have an absolute right to object to processing, including third-party monitoring, if this is for direct marketing purposes: IoT companies will have to immediately stop processing for such purposes.[51] It would be regrettable if IoT data controllers could invoke the limitations of the Things as an excuse to deprive citizens of the control over their data.

---

[44] On whether the lack of control can be overcome through data ownership see V. JANEČEK, "Ownership of Personal Data in the Internet of Things" *Computer Law & Security Review*, 2018, p. 1039.

[45] The problem of information asymmetry in the IoT has been analysed from a US consumer contracts' perspective by S.-A. ELVY, "Contracting in the Age of the Internet of Things: Article 2 of the UCC and Beyond" *Hofstra L. Rev.*, 2015, 44, p. 839.

[46] ARTICLE 29 WORKING PARTY, *op. cit.*, p. 6.

[47] Improve Digital Platform Privacy Policy, 3, last updated on 20 December 2018 <https://www.improvedigital.com/platform-privacy-policy/> accessed 27 May 2020, emphasis added.

[48] GDPR, recital 47.

[49] Art 5. The requirement applies all methods and techniques used to store information on a data subject's device or to gain access to information on said device. The draft e-Privacy Regulation is attempting to overcome the current cookie notice approach and shift to a consent expressed by means of browser' settings (Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC, COM/2017/10 final - 2017/03 (COD), recitals 22-24). Given the limitations of the Things, it will be crucial that they are set by default as not consenting to the use of cookies. It should be noted that the current version of the draft does not contain reference to expressing consent via browser settings (see Council of the EU, 6 March 2020 no 6543/20 - 2017/0003(COD)).

[50] GDPR, art 21(1).

[51] GDPR, art 21(2)-(3).

A second, closely interwoven, issue has to do with the quality of the IoT user's consent.[52] From a technical point of view, consent in the IoT is problematic mainly for two reasons.[53] A first technical issue is that '(r)esource heterogeneity and limitations are found in connectivity, computational power, storage,'[54] as well as in Input/Output, which refers to devices used to communicate with computers, e.g. keyboards and monitors. As an example of such limitations, one can think of the limited size of Things' screens or the lack of screens. This limitation renders compliance with pre-contractual duties of information difficult. This limitation makes it also hard for IoT companies to provide appropriate privacy notices, and for their users to input privacy choices.[55] Accordingly, it has been convincingly argued that the 'existing privacy frameworks that rely heavily on a notice and choice model [does] not effectively safeguard consumers in the IoT setting.'[56] A second technical issue that makes consent in the IoT problematic is device identity. Traditional authorisation systems used to decide whether a requester of a resource has sufficient permissions are not 'fully applicable to the IoT.'[57]. A privacy policy needs to state exactly who interacts with what data, when, where, how, and why. This conflicts with the objective of easy-to-understand policies, especially in the IoT context. Pointing out all possible data interactions is challenging at best, and detrimental to understanding at worst. However, consent can be regarded as 'informed' only if the user has sufficient knowledge of the risks and benefits of disclosing information to make a reasonable evaluation.[58]

Consent must be informed, which does not seem to be the case in the IoT where users are unlikely to be aware of their Things' processing activities. Informed consent has been regard as impossible because of IoT's features such as sensor fusion and 'the near impossibility of truly de-identifying sensor data.'[59] Therefore, data controllers had better not rely on consent as a valid justification for processing.[60] This is also due to the fact that Things are ubiquitous and barely noticeable, which makes the idea of informed consent untenable. This is all the more true when data controllers state that the alternative to

[52] See e.g. Y. O'CONNOR ET AL., "Privacy by Design: Informed Consent and Internet of Things for Smart Health" *Procedia Computer Science*, 2017, 113, p. 653.: 'the first phase for universal usability of IoT within the smart health domain is to ensure that digital health citizens […] are fully aware of what they are consenting to when they register an account with such technological artefacts' and accordingly suggest privacy by design solutions.'

[53] C. SENGUL, "Privacy, Consent and Authorization in IoT", *2017 20th Conference on Innovations in Clouds, Internet and Networks (ICIN)* (IEEE 2017) <https://ieeexplore.ieee.org/document/7899432/> accessed 3 June 2020.

[54] ibid.

[55] On the lack of opportunity in a smart city environment for the giving of meaningful consent see L. EDWARDS, "Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective" *EDPL*, 2016, 2, p. 28.

[56] S.-A. ELVY, "Commodifying Consumer Data in the Era of the Internet of Things" *Boston College Law Review*, 2018, 59, p. 423.

[57] Referring to Access Control Lists and Role-Based Access Control, SENGUL, *op. cit.*, p. 320.

[58] R.H. SLOAN, R. WARNER, "Beyond Notice and Choice: Privacy, Norms, and Consent" *Journal of High Technology Law*, 2014, 14, p. 370.

[59] S.R. PEPPET, "Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent" *Texas Law Review*, 2014, 93, p. 85.

[60] ARTICLE 29 WORKING PARTY, *op. cit.*, p. 7.

consenting is renouncing certain services or features.[61] Consent must be freely given, and this does seem the case here. Especially because, when assessing whether consent is freely given, account has to be given to whether the performance of the contract 'is conditional on consent to the processing of personal data that is not necessary for'[62] said performance. For example, IoT companies cannot make the functioning of their virtual assistant conditional to consenting to interest-based advertising.[63]

The requirements for consent to be informed and freely given is not an innovation of the GDPR. The Data Protection Directive already imposed these requirements, alongside requiring consent to be specific and unambiguous.[64] Specific means that consent must be given in relation to 'one or more specific purposes'[65] and that a data subject has a choice in relation to each of them. This requirement is closely interwoven with the principle of purpose limitation.[66] Therefore, IoT's repurposing challenges both. Under the Data Protection Directive, 'unambiguous' meant the 'indication of wishes by which the data subject signifies his agreement to personal data relating to him being processed.'[67] In theory, this meant that opt-out mechanisms (e.g. pre-ticked boxes) would have complied with this requirement. In practice, the Article 29 Working Party clarified that a clear affirmative action was needed.[68] This position was finally adopted by the GDPR.[69] Silence, pre-ticked boxes, or inactivity cannot be regarded as meeting the standard.[70] Accordingly, IoT companies that give users the possibility 'to opt out of certain other types of data processing by updating your settings on the applicable (…) device'[71] are not relying a valid consent.[72]

The innovations of the GDPR as far as consent is concerned are – alongside clearer rules regarding the pre-existing requirements – the new requirements of granularity, ease of withdrawal, and demonstrability. The heightened standard for consent under the GDPR and the 'increase of personal data collection, use and re-use, will make consent a major

[61] Cf. N. TUSIKOV, "Regulation through 'Bricking': Private Ordering in the 'Internet of Things'" *Internet Policy Review*, 2019, 8.
[62] GDPR, art 7(4).
[63] However, see Amazon Interest-Based Ads policy whereby 'You can choose not to receive interest-based ads from Amazon. You will still see ads, but they will not be based on your interests.' It is possible to speculate that in doing so the company relies on its legitimate interest, rather than consent.
[64] Data Protection Directive, arts 2(h) and 7(a).
[65] EUROPEAN DATA PROTECTION BOARD, "Guidelines 05/2020 on Consent under Regulation 2016/679" v 1.1 13, 2020.
[66] Ibidem 14.
[67] Data Protection Directive, art 2(h).
[68] ARTICLE 29 WORKING PARTY, "Opinion 15/2011 on the Definition of Consent" *WP187 26*, 2011. This opinion was replaced by ARTICLE 29 WORKING PARTY, "Guidelines on Consent under Regulation 2016/679" *WP259 rev.01*, 2018. More recently, they have been superseded by EUROPEAN DATA PROTECTION BOARD, *op. loc. cit.*
[69] GDPR, Art 4(11).
[70] GDPR, recital 32.
[71] Amazon Privacy Notice, last updated 22 March 2019 <https://www.amazon.co.uk/gp/help/customer/display.html?nodeId=201909010> accessed 9 June 2020.
[72] It must be said that Amazon tend to rely, as a legal basis for processing, on legitimate interest, contractual necessity, and legal obligation. However, 'We may also ask for your consent to process your personal information for a specific purpose that we communicate to you.' (Amazon Privacy Notice).

problem for IoT players.'[73] First, 'granular' means that there should be separate consent options for different types of processing and, if the data subject's consent is given in the context of a written declaration which also concerns other matters, 'the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.'[74] Practically, this means that IoT companies cannot bury consent in a long document that deals also with non-privacy related matters (e.g. the terms of service).[75] Second, IoT users should be free to withdraw their consent at any time and with the same ease that characterised the giving of the consent.[76] This means that when consent is obtained via electronic means 'through only one mouse-click, swipe, or keystroke,'[77] IoT companies cannot impose more cumbersome procedures to withdraw consent. Third, consent must be demonstrable; indeed, the controller – the IoT company in our scenario – must be able to 'demonstrate that the data subject has consented to processing of his or her personal data.'[78] This is an application of the overarching principle of accountability that the GDPR introduced to make clear that compliance as such is not enough: controllers must keep accurate records of their processing activities and of the ways they comply with the GDPR.[79] Accordingly, IoT companies must retain proof of a valid consent as long as the processing lasts, and after the processing ends, for as long as it is necessary for compliance with a legal obligation or for the exercise of legal claims.[80] The lack of accountability in the IoT precludes meaningful engagement by users with their personal data and 'poses a key challenge to creating user trust in the IoT and the reciprocal development of the digital economy.'[81] Accountability is rendered difficult by IoT's inadequate consent mechanisms, opaque distributed data flows, and lack of adequate interfaces; therefore, IoT companies have to invest sufficient resources in finding creative solutions to demonstrate compliance.[82]

In the context of wearables and consent to the processing of sensitive personal data, then, it has been observed[83] that a too rigid interpretation of consent may stifle innovation; accordingly, self-regulation has been recommended as a solution. However, self-regulation does not appear the best regulatory approach when private entities have incentives to behave in ways that are not conducive to the common good. Conversely, at least some of the issues of consent in the IoT can be overcome by moving 'past reliance on contractual

[73] L. TANCZER ET AL., 'IoT and Its Implications for Informed Consent' *PETRAS IoT Hub, STEaPP: London*, 2017 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3117293> accessed 3 June 2020.
[74] GDPR, art 7(2).
[75] INFORMATION COMMISSIONER'S OFFICE, "Lawful Basis for Processing: Consent" v 1.0.65 4, 2018.
[76] GDPR, art 7(3).
[77] EUROPEAN DATA PROTECTION BOARD, *op. cit.*, p. 23.
[78] GDPR, art 7(1).
[79] GDPR, art 5(2).
[80] GDPR, art 17(3)(b),(e); EUROPEAN DATA PROTECTION BOARD, *op. cit.*, pp. 22–23.
[81] Lachlan URQUHART, Tom LODGE and Andy CRABTREE, 'Demonstrably Doing Accountability in the Internet of Things' (2019) 27 International Journal of Law and Information Technology 1.
[82] One such solution is the so-called IoT Databox presented ibid 15.
[83] Syagnik BANERJEE, Thomas HEMPHILL and Phil LONGSTREET, 'Wearable Devices and Healthcare: Data Sharing and Privacy' (2018) 34 The Information Society 49.

T&C (and) use the concept of trajectories.'[84] The concept of trajectories has been developed by human-computer interaction (HCI) scholars.[85] HCI is a domain of technology design that 'prioritises understanding the social context of technology, questioning the interactions and relationships between end users and technology.'[86] Trajectories are a 'conceptual framework for understanding cultural user experiences,'[87] and for designing interactive user experiences. What trajectories have in common, is that 'they take their participants on journeys (that) may pass through different places, times, roles and interfaces.'[88] IoT designers could adopt this framework to embed a GDPR-compliant in the users' trajectory thus improving the overall experience. Trajectories' designers have to consider factors such as the temporal nature, the actors involved, the physical space itself and the computer interfaces.'[89] This means, for example, that as opposed to providing all information upfront, 'information can be spread over the lifetime'[90] of the user-Thing relationship. This multidisciplinary approach is certainly promising, although it is still unclear how to provide incentives to push IoT companies to adopting HCI principles in the design of their GDPR compliance.

Third, in the IoT there are intertwined data protection issues of repurposing of original processing[91] and the inferences derived from data.[92] We have already dealt with repurposing. Suffice to add that repurposing is also made possible by the so-called sensor fusion, that consists in 'combining sensor data or data derived from different sources in order to get better and more precise information than would be possible when these sources are working in isolation.'[93] More pressing is the question of inferences, whose status as personal data is contested.[94] The IoT requires pervasive collection and 'linkage of user data to provide personalised experiences based on potentially *invasive inferences*.'[95] The joint operation of IoT-produced big data, improved data mining techniques, and the combination of data from multiple sources leads to the creation of highly valuable inferences about the user's behaviour and vulnerabilities. This is problematic for a twofold reason. Analytics is moving from being merely predictive, to give IoT companies the power to change the way the individual actually behaves. For example, there is evidence that people censor

[84] Lachlan URQUHART and Tom RODDEN, 'New Directions in Information Technology Law: Learning from Human–Computer Interaction' (2017) 31 International Review of Law, Computers & Technology 150, 164.
[85] Steve BENFORD AND OTHERS, 'From Interaction to Trajectories: Designing Coherent Journeys through User Experiences', *Proceedings of the 27th international conference on Human factors in computing systems - CHI 09* (ACM Press 2009) <http://dl.acm.org/citation.cfm?doid=1518701.1518812> accessed 9 June 2020.
[86] Urquhart and Rodden (n 95) 150.
[87] BENFORD AND OTHERS (n 96) 710.
[88] ibid 712.
[89] URQUHART and RODDEN (n 95) 161.
[90] ibid 162.
[91]Guido NOTO LA DIEGA, 'British Perspectives on the Internet of Things. The Clouds of Things-Health Use Case', *Internet of Things: Legal Issues and Challenges towards a Hyperconnected World* (Seoul National University 2015) 45.
[92] WACHTER, MITTELSTADT, *op. loc. cit.*
[93] ARTICLE 29 WORKING PARTY, *op. cit.*, p. 7, fn 6.
[94] WACHTER, MITTELSTADT, *op. loc. cit.*
[95] S. WACHTER, "The GDPR and the Internet of Things: A Three-Step Transparency Model" *Law, Innovation and Technology*, 2018, 10, p. 266.

themselves when they know that they feel that they are being watched.[96] Moreover, these inferences may not necessarily be regarded as personal data, which would bring the processing outside of the scope of the GDPR. If this thesis prevails, IoT companies may side-step the principle of purpose limitation and re-use inferred data for purposes that go beyond the original purpose for which data had been collected. Moreover, users could not invoke the right to rectify[97] inaccurate and unreasonable inferences, which is alarming since inferences are unverifiable and 'create new opportunities for discriminatory, biased, and invasive decision-making.'[98] Accordingly it has been argued[99] that a new 'right to reasonable inferences' is needed to help close the accountability gap currently posed by high-risk inferences. The proposal has two drawbacks. First, it is characterised by the same rights-based approach that negatively affects the GDPR: it leaves the effectivity of data protection to the initiative of the individual citizens, that has scares resources and knowledge to bring a lawsuit against IoT big tech.[100] Second, albeit imperfect, the GDPR provides tools against abuses regarding inferred data. Indeed, although the right not be subject to automated decisions[101] is unlikely to apply to inferences, lacking a significant 'decision', the rules on profiling apply regardless of a solely automated decision.[102] Profiling consists of any form of automated processing of personal data to analyse an individual's personality, behaviour, interests and habits to make predictions or decisions about them.[103] The definition is broad enough to encompass most inferences. And indeed, as noted by the Article 29 Working Party, profiling is 'often used to make predictions about people, using *data from various sources to infer something* about an individual, based on the qualities of others who appear statistically similar.'[104] This means that IoT companies whose business model relies on inferences have to actively inform the data subject about profiling and carry out a Data Protection Impact Assessment.[105] Moreover, since inferences are personal data, the principle of accuracy will apply.[106] Therefore, IoT companies have to put in place have appropriate processes in place to check that personal data, including inferences, is correct and not misleading.[107] The importance of accurate inferences is also underlined by the Council of Europe that stress importance of data

[96] J.W. PENNEY, "Chilling Effects: Online Surveillance and Wikipedia Use" *Berkeley Technology Law Journal*, 2016, 31, p. 117.
[97] GDPR, art 16.
[98] WACHTER, MITTELSTADT, *op. cit.*, p. 494.
[99] Ibidem.
[100] See R. ALLSOPP, "Levelling the Odds? Big Data Analytics in the Online Gambling Industry and the Application of the GDPR" in M.M. CARVALHO (ed), *Law & Technology. E.Tec Yearbook*, University of Minho, Minho, 2018, p. 135.
[101] GDPR, art 22.
[102] ARTICLE 29 WORKING PARTY, "Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679" *WP251rev.01*, 2018, p. 7.
[103] GDPR, art 4(4).
[104] ARTICLE 29 WORKING PARTY, "Guidelines on Automated Individual Decision-Making", cit., p. 7. Emphasis added.
[105] INFORMATION COMMISSIONER'S OFFICE, "Automated Decision-Making and Profiling" v. 1.1.49, 2018, pp. 4–5.
[106] GDPR, art 5(1)(d).
[107] See INFORMATION COMMISSIONER'S OFFICE, *Guide to the General Data Protection Regulation*, London, ICO, 2019, p. 33.

quality and recommends that the data controller 'periodically and within a reasonable time reevaluate the quality of the data and of the statistical inferences used.'[108] Accordingly, IoT companies should put in place appropriate measures to correct data inaccuracy factors and limit the risks of errors inherent in profiling.

Fourth, there are limitations on the possibility to remain anonymous when using Things; this is problematic since anonymisation is identified as a best practice in data processing, especially when profiling.[109] The IoT makes robust anonymisation difficult for a fourfold reason. First, Things and IoT systems produce an abundance of data as exemplified by the fact that UK smart meters generate 21.2 billion megabytes of data each year.[110] Second, this data is more granular because of the possibility to recombine data coming from multiple sources, also thanks to more refined tracking techniques. For example, using signals that can be heard from a user's Things but not from the user themselves, IoT traders can map all the Things used by the same user, which makes cross-device tracking easier.[111] Third, the data produced by Things and IoT systems provides information that relates the most intimate aspects of an individual's life. This is because they are ubiquitous and they can access the most private spaces, including the home and the body. Finally, Things that are in close proximity to the data subject (e.g. wearables) result in the availability of stable identifiers (e.g. multiple MAC addresses),[112] that lead to the creation of a unique fingerprint.[113] In light of the above – and thanks the ensuing data power[114] that IoT companies hold – anonymous data can be easily reconnected to individuals.[115]

Finally, and this is an issue that the Article 29 Working Party overlooked, there is the problem of data appropriation.[116] IoT companies attempt to appropriate and control both the algorithms that underpin the IoT system and the data that this system produces. Leveraging a portfolio of big data and intellectual property rights (especially trade secrets), IoT companies put in place practices that can negatively affect citizens, who are often unaware of them due to a technical and legal secrecy. 'Technical' secrecy results from the opacity of the algorithms that underpin the IoT, especially when AI-enabled. 'Legal'

---

[108] COUNCIL OF EUROPE, *The Protection of Individuals with Regard to Automatic Processing of Personal Data in Context of Profiling: Recommendation CM/Rec(2010)13 Adopted by the Committee of Minsters of the Council of Europe on 23 November 2010 and Explanatory Memorandum*, Council of Europe, Strasbourg, 2011, p. 11.

[109] INFORMATION COMMISSIONER'S OFFICE, *Guide*, cit., p. 157.

[110] M. WILD, M. THORNE, "A Price of One's Own. An Investigation into Personalised Pricing in Essential Markets" *Citizens Advice*, 2018.

[111] H. JIN, C. HOLZ, K. HORNBAEK, "Tracko: Ad-Hoc Mobile 3D Tracking Using Bluetooth Low Energy and Inaudible Signals for Cross-Device Interaction" *Proceedings of the 28th Annual ACM Symposium on User Interface Software & Technology*, ACM, New York, 2015, p. 147.

[112] Media access control (MAC) address is the hardware address of a device connected to a network. Jeff RUTENBECK, *Tech Terms: What Every Telecommunications and Digital Media Professional Should Know*, Routledge, Abingdon, 2012, p. 161.

[113] ARTICLE 29 WORKING PARTY, *op. cit.*, p. 8.

[114] O. LYNSKEY, "Grappling with 'Data Power': Normative Nudges from Data Protection and Privacy" *Theoretical Inquiries in Law*, 2019, 20, p. 189.

[115] L. EDWARDS, M. VEALE, "Slave to the Algorithm: Why a Right to an Explanation Is Probably Not the Remedy You Are Looking For" *Duke L. & Tech. Rev.*, 2017, 16, p. 18.

[116] S. ZUBOFF, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, New York, 2019.

secrecy, in turn, come from a combination of trade secrets, proprietary software and contracts that keep IoT data practices secret. Thanks to the data power that IoT big players hold, they can take advantage of their dominant position to impose contracts that purport to justify unfair and opaque practices, including the appropriation and re-use of personal as well as non-personal data. This proprietary strategy can harm citizens in manifold ways. It can affect their privacy, because it allows for surreptitious forms of monitoring and surveillance. It can also affect their autonomy and self-determination because IoT data allows companies to exploit users' biases and vulnerabilities to manipulate them. It can even affect their dignity, when IoT data includes protected characteristics that allow companies to discriminate against certain categories of citizens.[117] For example, following the brutal killing of George Floyd, tech companies started announcing that they would stop selling facial recognition software to law enforcement because it is inherently biased against BAME people.[118] However, the same companies often kept entering into agreements with the police allowing for forms of biased policing and surveillance. This was well illustrated by Amazon's Ring – 'smart' home doorbell – that allowed (and still do) users to share concerning video footage with the police: reports[119] have found that a disproportionate number of incidents involve people of colour.

III. Trade secrets can cover IoT data and algorithms

Keeping strategic and commercially valuable information undisclosed to maintain a competitive advantage over competitors is the oldest form of protection[120] that market operators have traditionally relied on at a local level. Loss of such a competitive advantage due to leaks from former or current employees or collaborators or cyber-attacks can lead to very substantial estimated damage[121]. Internationally, Article 39 of TRIPs introduced trade secrets as a complementary (or alternative)[122] protection among Intellectual Property

[117] It has been noted that the fact that Things tell us more and more about ourselves and each other will permit racial, economic, as well as new forms of discrimination. PEPPET, *op. loc. cit.*

[118] E. BIRNBAUM, I. LAPOWSKY, "Amazon, Facing Pressure, Won't Provide Facial Recognition to Police for a Year" (*Protocol*, 10 June 2020) <https://www.protocol.com/amazon-facial-recognition-police> accessed 16 June 2020.

[119] C. HASKINS, "Amazon's Home Security Company Is Turning Everyone Into Cops" (*Vice*, 7 February 2019) <https://www.vice.com/en_us/article/qvyvzd/amazons-home-security-company-is-turning-everyone-into-cops> accessed 16 June 2020.

[120] M. LEMLEY, "The Surprising Virtues of Treating Trade Secret as IP Rights", *Stanford Law Review*, 2008, p. 311.

[121] Trade secret law typically works far better for business information than private data. One might indeed expect the default contracts may not adequately protect the users or consumers—though privacy or consumer protection laws may impose limits on contractual freedoms that include minimum guarantees of confidentiality. D. GERVAIS, "Exploring the Interfaces Between Big Data and Intellectual Property Law", *JIPITEC* 2019, p. 3.

[122] Directive 2016/943/EU of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure ('Trade Secrets Directive') O.J. L 157, 15.6.2016, p. 1, recital 1, would suggest that this is a complementary form of protection, according to A. OTTOLIA, "Il D. Lgs n. 63/18 di attuazione della direttiva sulla protezione dei segreti commerciali fra tutela e bilanciamenti", *NLCC*, 2019/5, p. 1091, who refers to other authors sharing this position. However, on the one hand the Recital 1 does not expressly refer to this complementarity. In this sense, T. HOEREN, "The EU Directive on the Protection of Trade Secrets and its Relation to Current Provisions in Germany", *JIPITEC*, 2018, p. 138, refers to Recital 2 and indicates that the protection can be either complementary or alternative. On the other hand, a factual element is worthy to be

Rights (IPRs) for protecting information, which may or may not qualify for or enjoy patent or other forms of protection. This extension aimed to limit leaks-related risks and introduce a framework to foster development, exchange and use innovation knowledge. This article has been recently implemented in the EU by Directive 2016/943/EU, based on Article 114 TFEU and thus aimed at harmonising civil actions related to trade secrets misappropriation[123]. More broadly speaking, the goal of this text is to boost innovation, competition as well as research and circulation of knowledge, without jeopardizing (among others) consumer protection[124]. Member states have transposed this Directive at the national level in different ways and times. As to the jurisdictions we selected, Italy introduced Article 3.2 of the Decreto Legislativo 11 May 2018 n. 63, modifying to a limited extent Articles 98 and 99 of the Industrial Property Code.[125] In turn, France implemented it on 30 July 2018, with Act 2018-670, which introduces new clauses in the Business Code[126]. Notwithstanding Brexit, the UK chose to respect its obligation via the Trade Secrets Regulations[127], which came into force on 9 June 2018[128].

According to these sources, the subject matter of trade secrets protection is information as well as know-how[129]. More precisely, both these elements are protectable when they fulfill the three following requirements[130]: first, they are "not generally known or readily accessible to persons within the circles that normally deal with the kind of information in question"[131]. Secondly, their secrecy must provide them a commercial value[132]. Thirdly, the

---

noted: it is hard to see how Small and Medium Enterprises (SMEs) could see it as a complementary and not an alternative legal tool.

[123] *Supra*, note 66. In a comparative perspective, on the US legal framework: M. LEMLEY, *op. loc. cit.*; S. SANDEEN, "The Limits of Trade Secret Law" in R. DREYFUSS, K. STRANDBURG (eds.), *The Law and Theory of Trade Secrecy. A Handbook of Contemporary Research*, Cheltenham, Edward Elgar, 2011, p. 538. For some information in a comparative perspective see G. SURBLYTÉ, "Enhancing TRIPS: Trade Secrets and Reverse Engineering" in H. ULLRICH, R. HILTY, M. LAMPING, J. DREXL (eds.), *TRIPS plus 20. From Trade Rules to Market Principles*, Berlin, Springer, 2016, p. 725; and C. SAPPA, "How Data Protection Fits with the Algorithmic Society via Two Intellectual Property Rights, cit., p. 135.

[124] See Trade Secrets Directive, recitals 16 and 21.

[125] Decreto legislativo 10 February 2005, n. 30 "Codice della proprietà industriale" (hereinafter also 'Italy's Industrial Property Code').

[126] Code de commerce (Business Code), arts L 151-1 ff.. On this see J.-C. GALLOUX, "Secret des affaires et propriété intellectuelle", *Dalloz IP/IT*, 2018, p. 666.

[127] Trade Secrets (Enforcement, etc.) Regulations SI 2018/597.

[128] T. APLIN, R. ARNOLD, "UK implementation of the Trade Secret Directive" in J. SCHVOSBO, T. MINSSEN,, T. RIIS (eds.), *The Harmonisation and Protection of Trade Secrets in the EU. An Appraisal of the EU Directive*, Cheltenham, Edward Elgar, 2019, p. 65.

[129] On the subject matter of protection: J. REICHMAN, "Charting the Collapse of the Patent-Copyright Dichotomy: Premises for a Restructured International Intellectual Property System", *Cardozo Art & Entertainment* 1995, p. 475.

[130] In lack of these requirements the protection granted may still be the one offered to confidential information, in particular in presence of an express agreement On this see E. JOHNSON, "Trade Secret Subject Matter", *Hamline Law Rev.*, 2010, pp. 563 and 565; and J. REICHMAN, "Overlapping Proprietary Rights in University Granted Research Products: The Case of Computer Programs", *Columbia Journal Law & Arts*, 1992, p. 51.

[131] Italy's Industrial Property Code, art 98 still refers to information that is not notorious or easily accessible by experts in the field. Of course, in case of conflict the Trade Secrets Directive shall prevail.

[132] A. A. WENNAKOSKI, "Trade Secrets Under Review: A Comparative Analysis of the Protection of Trade Secrets in the EU and in the US", *EIPR*, 2016, p. 154, suggests that this requirement is easy to be fulfilled. In addition, see Council of the EU, "Opinion 9870/14 PI 67 CODEC 1295" (*Consilium*, 26 May 2014) <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%209870%202014%20INIT> accessed 4 May 2020, spec. 15 and recital 8, stating that the commercial value of the information may be actual or potential.

person who is lawfully in control[133] of the information or know-how needs to have an express or at least a recognizable intention to keep it secret[134], via an appropriate implementation of technical, organizational and contractual barriers[135], such as lockers, encryption measures, regularly changing passwords, confidentiality agreements, non-competition clauses, which would impede an easy access to the information. It should be noted, however, that questions may arise if encrypted information is posted online. It will not necessarily count as confidential because "Anyone with the necessary skill to de-crypt had access to the information. The fact that only a few have those skills is (…) neither here nor there. Anyone can acquire the skills and, anyway, a buyer is free to go to a man who has them"[136]. In the same sense one could not consider secret the information that is embodied in an object that, being in the public domain, can be easily accessed through reverse engineering[137]. Accordingly, one may argue that the data and the algorithms that are embodied in Things are not secret, as long as they can be easily accessed by means of reverse engineering or decrypted. However, courts have become in more recent times amendable to the idea of considering Thing-embedded algorithms as secret[138].
Other papers have argued that – at least in principle – trade secrets protection[139] applies to IoT data[140], which are mainly the outcome of automated processes used for the collection, archiving and any further elaboration of data. Therefore, it would cover data produced and

---

The current Article 2(1)(b) of the Trade Secrets Directive does not refer to potential commercial value, however recital 14 does. At the national level, the Directive was transposed in a different way in France and in Italy. In France, the Code de Commerce states that both actual and potential value of the information are taken into account to assess the protectability of it (art L 151-1). In Italy, the Legislative Decree of 11 May 2018 n. 63 merely refers to the economic value of the secret information (art. 3(2)). However, this would not be against the EU legislator instructions according to A. OTTOLIA, "Il D. Lgs n. 63/18", cit..

[133] Trade Secrets Directive, recitals 7, 12 and art 2(1)(c).

[134] G. SURBLYTÉ, "Enhancing TRIPS", cit., explains that this requirement is not in the TRIPs, art 39.

[135] G. PSAROUDAKIS, "Trade Secrets in the Cloud", *EIPR* 2016, p. 344, in principle, a higher diligence is expected from the owner of the secret information stored in a cloud, and in any case an exclusion (or limitation to a certain extent) of liability clause of the cloud provider would not be aligned nor consistent with reasonable efforts to keep the information secret.

[136] Mars v Teknowledge [2000] FSR 138, 149, dealing with the common law of breach of confidence; therefore, it does not necessarily mean that encrypted information cannot account as confidential under the Trade Secrets Directive.

[137] Saltman Engineering Co v Campbell Engineering Co (1948) 65 R.P.C. 203

[138] Volkswagen v Garcia [2013] EWHC 1832 (Ch), where the court granted an interim injunction to prevent the disclosure of an algorithm. This algorithm was embedded in a car's immobilizer and the defendants had accessed it by reverse engineering a computer program that they had found online. The court did not consider *Saltman* and ignored the issue of whether, once decrypted, the algorithms could still be regarded as secret. Moreover, a crucial role was played by the practical consideration that the disclosure may have led to mass car theft. Nonetheless, *Volkswagen v Garcia* remains an important victory for those who consider IoT-embedded data and algorithms as secret. See also Ackroyds v. Islington Plastics [1962] RPC 97, 104, whereby if the information in the public domain needs reverse engineering, it has to be treated as relatively secret

[139] Trade secrets would be complementary to other legal forms of protection, as explained by A. OTTOLIA, *Big Data e innovazione computazionale*, Turin, Giappichelli, 2017; or to a *de facto* protection, as per M. RICOLFI, "IoT and the Age of Antitrust", *Concorrenza e Mercato*, 2017, p. 214.

[140] See A. OTTOLIA, *Big Data e innovazione computazionale*, cit.; C. SAPPA, "IoT: What does Trade secrets have to do in an Interconnection-based paradigm?", *EIPR*, 2018, p. 518; ID., "Le secret des affaires dans la société algorithmique: une presence profitable", *RTDcom*, 2020, p. 847. *Contra*: J. DREXL, "Designing Competitive Markets for Industrial Data – Between Propertization and Access", *JIPITEC*, 2016, p. 257; A. WIEBE, "Protection of Industrial Data – A New Property Right for the Digital Economy", *GRUR Int*., 2016, p. 877.

managed by the well-known IoT devices Dash Button and Echo. Even if the Trade Secrets Directive does not expressly refer to data resulting from a machine-to-machine process, an extensive interpretation of this text, which includes them in the protectable subject matter together with data generated in other and more traditional ways, has to be followed. Indeed, this position is aligned with the fundamental principle of non-discrimination, which impedes an unjustified diversity of treatment for data depending on their nature[141].

It has to be added that in the IoT framework, data, including raw data, may seem of trivial value if considered at the time of collection and in isolation. Valuable knowledge may derive from data mining and aggregation of data that is accumulated over time from multiple sources. Isolated data as such may not necessarily have any commercial value, but they can be aggregated and combined in ways that produce such value. This means that in the context of big data analysis, an individual piece of information may appear deprived of value and thus non protectable under Recital 14 of the Trade Secrets Directive[142]. However, substantial value may arise from the correlation of such (trivial) information with other data. With big data, including IoT data, trivial information can have economic value when there is enough trivial information that is put together and analysed. This begs the question whether we should extend trade secrets protection also to databases obtained by aggregating data initially gathered by humans or artificial techniques.[143] Should this diachronically created information have a potential commercial value, it would certainly deserve protection[144].

IoT data that are unable to meet the aforementioned requirements are likely to fall outside the protection. For instance, trade secrets cover information that is not generally known or readily ascertainable in one field; however, they do not cover unavailable data. This is related to the so-called black box in the IoT, i.e. rooms where decision-making model rules may remain unknown and undecryptable even to their owner. It is not possible to assume that trade secrets cover such an automated information. In order to have the information protected, it is necessary to run tests able to confirm that the unknown decision-making model works in a way that is different from what is known, no matter its specific analytical content[145].

It is disputed whether trade secrets are a conduct-based liability rule[146], or an absolute right.[147] Regardless, it can be accepted that trade secrets do not grant any

---

[141] See however M. BERTANI, "Proprietà intellettuale e nuove tecniche di appropriazione delle informazioni*"*, *AIDA 2005*, 2006, p. 322, who explains that some jurisdictions may have foreseen different kinds of protection for different data. In Italy, before 2010, non-patentable information was potentially protected by unfair competition under the Civil Code, art 2598(3), but not by trade secrets under the Industrial Property Code, arts 98 and 99.

[142] H. ZECH, "Data as tradeable commodity" in A. DE. FRANCESCHI (ed.), *European contract law and the digital single market*, Cambridge, Intersentia, 2016, p. 63, who criticizes the recital.

[143] In a different, but complementary perspective, on the sui generis protection on IoT databases see C. SAPPA, "How Data Protection Fits with the Algorithmic Society via Two Intellectual Property Rights", cit.; G. NOTO LA DIEGA, "Artificial Intelligence and Databases", cit., p. 93.

[144] This would comply with the Trade Secrets Directive, recital 14 and art 2. In this sense see G. MALGIERI, " 'Ownership' of Customer (Big) Data in the European Union: Quasi-Property As Comparative Solution?", *J Internet L*, 2016, p. 3.

[145] A. OTTOLIA, "Il D. Lgs n. 63/18", cit.. *Contra*, T. APLIN, "The limits of trade secret protection in the EU", in S. SANDEEN, C. RADEMACHER and A. OHLY (eds) Research Handbook on Information Law and Governance (Edward Elgar, Cheltenham, forthcoming 2021), currently available at SSRN: https://ssrn.com/abstract=

[146] J. REICHMAN, "How Trade Secrecy Law Generates Innovative Know-How" in R. DREYFUSS, K. STRANDBURG (eds.), *The Law and Theory of Trade Secrecy*, Cheltenham, Edward Elgar, 2011, p. 185. See

exclusive right[148], unlike other IPRs. It protects certain information against unlawful extraction[149], while independent discoveries of the same information do not consist in an unlawful acquisition of the information and thus do not lead to any infringement of the trade secrets protection. As well as independent discoveries, third parties reverse engineering initiatives by honest means are able to put an end to its existence[150].

IoT algorithms processing aggregated data as well as their output can benefit from the protection of trade secrets. Accordingly, their unauthorised use is possible under trade secrets' limitations and exceptions. These exceptions and limitations as per Article 5 of the Trade Secrets Directive create room for considerable consumer freedom. Some authors consider exceptions and limitations as aimed at ensuring the interest of circulation of knowledge[151], while others think they merely serve more specific interests[152]. Some authors recognise the emphasis the Directive puts on such exceptions and limitations; however, they regard as unclear the mechanisms for assessing unjustified interferences between trade secrets and the right to freedom of expression and information, or legitimate interest[153].

France has expressly implemented some exceptions of the Trade Secrets Directive. Its Article 5(a) states that defendants can claim that the acquisition, use or disclosure of the secret was carried out "for exercising the right to freedom of expression and information". This statement includes – and is not limited to – the freedom of the press. The French legislator made it particularly clear, since she clearly distinguishes the "*liberté d'expression et de communication*"[154] that is epitomised by the press freedom, and the "*liberté d'information*"[155] that refers to the citizens' right to access information. Alongside this exception, under Article 5(d) of the Trade Secrets Directive, it is a defence in a trade-secret-related dispute that the acquisition, use or disclosure was carried out "for the purpose of protecting a legitimate interest recognised by Union or national law". This has been expressly recognized in France too, where the breach of the trade secret is not actionable if it was obtained, used or disclosed "*(p)our la protection d'un intérêt legitime reconnu*"[156] by EU law or national law.

---

also H. ZECH, "A Legal Framework for a data economy in the European Digital Single Market: Rights to Use Data", *JIPLP*, 2016, p. 460, suggesting that trade secrets holder has the property-like traits as to the allocation of economic value. Know-how is at least factually transferable and thus can be economically exploited and also be the object of legal transactions. Accordingly, the possibility of undue enrichment is affirmed in case of an injury.

147 A. OTTOLIA, "Il D. Lgs n. 63/18", cit.

148 Trade Secrets Directive, recital 16.

149 This would mean: against honest commercial practices. On this K.M. SAUNDERS, "The Law and Ethics of Trade Secrets: A Case Study", *Cal. W. L. Rev*., 2006, p. 209.

150 As indicated by J. C. STEDMAN, "Trade Secret*", Ohio State Law J*., 1962, p. 4. This is correct, provided that no contractual restriction applies. See Recital 16 of the Trade Secrets Directive and G. SURBLYTÉ, "Enhancing TRIPS", cit., p. 740, where she refers to German law.

151 S. SERAFINI, "Luci e ombre della nuova disciplina del segreto commerciale", *Corr. Giur*., 2018, p. 1337. In addition, other measures may present an horizontal approach, such as the common law-based defence of public interest in the UK.

152 A. OTTOLIA, "Il D. Lgs n. 63/18", cit..

153 And this would impact the harmonization aim of the Trade Secrets Directive. T. APLIN, "The limits of trade secret protection in the EU", cit.

154 Code de Commerce, art 151-8(1). Italy and the UK did not implement this exception for the same reasons reported with regards to the legitimate interest exception.

155 Code de Commerce, art 151-8(1).

156 Code de Commerce, art 151-8(3).

Italy and the UK did not expressly implement any of the Trade Secrets Directive' exceptions. In Italy, it was felt that there was no need to implement such exceptions because the principles underpinning them are already guaranteed in the Italian legal system thanks to case law.[157] Similarly, the UK resolved the issue by declaring that the statutory protection under the Trade Secrets Regulations adds to – but does not replace – the common law of breach of confidence.[158] This means that it will be possible in trade secrets proceedings to invoke the public interest defence[159], which is a common law defence that applies when the breach of confidence was necessary for a legitimate public interest, for example safety and freedom of expression.[160] The only problematic aspect is that trade secret holders can bring an action for breach of confidence only where the relevant remedies and procedures "provide wider protection to the trade secret holder"[161]. This might be interpreted as meaning that, since the public interest defence weakens the holder's position, the common law of breach of confidence, including said defence, will not apply. However, we put forward another interpretation: the public interest defence will always be available to defendants in trade secrets proceedings. Indeed, Regulation 3(1) of the Trade Secrets Regulations set out the general principle whereby "(t)he acquisition, use or disclosure of a trade secret is unlawful where the acquisition, use or disclosure constitutes a breach of confidence in confidential information". The instrument subsequently provides more detailed rules that apply to potential claimants i.e. trade secret holders: they can only invoke the common law of confidence if it provides them with a stronger protection. Since no special rules apply to defendants, the general principle will prevail and they will be able to invoke the common law defence of public interest in trade secrets proceedings, regardless of whether it provides a stronger protection to the trade secret holder.

Moreover, the trade secrets' exceptions are not only implemented through the public interest defence; they are also implemented by virtue of various statutory provisions,[162] including the Human Rights Act 1998,[163] which ratified the European Convention on Human Rights (ECHR).[164] This includes the possibility to interfere with the right to privacy "for the protection of the rights and freedoms of others"[165]. There is no doubt that data protection is a legitimate interest recognised by both EU and national laws. This is exemplified by the fact that the right to data protection under the Charter of Fundamental Rights of the EU is directly effective in all Member States, as seen in *Vidal-Hall v Google Inc*.[166] The Charter has the same value as the foundational treaties of the

[157] A. OTTOLIA, "Il D. Lgs n. 63/18", cit..
[158] Trade Secrets Regulations, reg 3.
[159] Explanatory Memorandum to The Trade Secrets (Enforcement, etc.) Regulations 2018 and annexed Transposition Note.
[160] Lion Laboratoires Ltd v Evans [1985] QB 526; Attorney General v Guardian Newspapers (No.2) (HL) 1989 1 AC 109; Campbell v MGN Ltd (HL) [2004] 2 AC 457.
[161] Trade Secrets Regulations, reg (2)(a).
[162] Transposition Note to The Trade Secrets (Enforcement, etc.) Regulations 2018.
[163] This is the statute that incorporated the ECHR into the UK legal systems.
[164] Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4.11.1950, ETS 5.
[165] The Human Rights Act 1998 incorporate the ECHR, art 8.
[166] [2015] EWCA Civ 311. See also Judgement of 6 November 2018, C-569/16 and C-570/16, Stadt Wuppertal v Maria Elisabeth Bauer and others, EU:C:2018:871, paragraphs 84-86 Judgement of 6 November 2018, C-684/16, Max-Planck-Gesellschaft zur Förderung der Wissenschaften e.V. v Tetsuji Shimizu, EU:C:2018:874, paragraphs 73-75, where it was decided that Charter's provisions can have both vertical and horizontal direct effects if they are unconditional in nature, and mandatory. See, more widely, E. FRANTZIOU,

EU.[167] The same value is attached to the ECHR, which has been ratified by all the Member States. Equally, the GDPR being directly applicable in all Member States, confirms that data protection is at the very least a legitimate interest that is protected throughout the Union and internally.[168]

The overall question is whether these exceptions and other limits to the trade secrets protection are sufficient to provide some transparency, thus empowering consumers.

From a consumer's perspective, disclosure of information is a crucial element for ensuring transparency. The importance of transparency is recognized also in the IP field. Patent law's philosophy lies in the social contract whose obligations are the disclosure of information on the one hand (as epitomized by the sufficiency requirement),[169] and a strong protection for a valuable invention on the other.[170] The pace of inventions, also thanks to the use of AI-powered data mining, is increasing vertically and it is not matched by the slowness of the patent application procedure.[171] Moreover, not every new idea is patentable; for example, the European Patent Office regards algorithms as mathematical methods that are, as such, excluded from patentability.[172] Thus, trade secrets are often considered as a more viable option than patents, in particular in the IT field[173]. Subsequently, information disclosure is more marginal than it would be suitable. Because

---

The Horizontal Effect of Fundamental Rights in the European Union. A Constitutional Analysis, Oxford, Oxford University Press, 2019, especially chapter 4.

[167] Treaty on European Union (TEU), O.J. C 202, 7.6.2016, p. 13, art 6(1), as amended by the Treaty of Lisbon, O.J. C 306, 17.12.2007, p. 1. Under the TEU, art 6(2), the EU has to ratify the ECHR (see also Protocol (No 8) relating to Article 6(2) of the TEU, O.J. C 326, 26.10.2012, p. 273). The EU have not ratified the ECHR yet because the CJEU has opined that the draft Accession Agreement of the EU to the ECHR, finalised on 5 April 2013, does not preserve the specific characteristics of the EU and does not make sure that the accession will not affect the EU's competences and powers. See Opinion 2/13 of 18 December 2014, ECLI:EU:C:2014:2454. The negotiations are ongoing and, if successful, EU citizens will be able to sue EU institutions for breach of the ECHR. However, the ECHR are already protected in the EU, and the Charter of Fundamental Rights of the EU provides a level of human rights protection that is equivalent to the ECHR. See EECKHOUT, Piet. "Opinion 2/13 on EU accession to the ECHR and judicial dialogue: Autonomy or autarky." Fordham Int'l LJ 38 (2015): 955; P. LEMMENS, "The Relation between the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights–Substantive Aspects." *Maastricht Journal of European and Comparative Law*, (2001/8, p. 49.

[168] Even after Brexit, the GDPR is still applicable in the UK because it has been incorporated by the Data Protection Act 2018. See more widely MOEREL, Lokke, and Ronan TIGNER. "Data Protection Implications of Brexit." Eur. Data Prot. L. Rev. 2 (2016): 381.

[169] Under the European Patent Convention, art 83, "The European patent application shall disclose the invention in a manner sufficiently clear and complete for it to be carried out by a person skilled in the art".

[170] This approach is particularly clear in Eldred v Ashcroft (2003) 537 US 186. However, the representation of the patent system as a form of social contract is criticised by S. GHOSH, "Patents and the Regulatory State: Rethinking the Patent Bargain Metaphor after Eldred", *Berkeley Technology Law Journal*, 2004, p. 1315.

[171] Cf. C. SHAPIRO, "Navigating the patent thicket: Cross licenses, patent pools, and standard setting", *Innovation policy and the economy*, 2000, p. 119.

[172] European Patent Convention, arts 52(2)(a) and 52(3)). In G 0003/08 (Programs for computers) of 12.5.2010, EP:BA:2010:G000308.20100512 [13.5.1], the European Patent Office's Boards of Appeal accepts that some consider algorithms as a procedure to make a machine carry out a certain task, thus involving technical considerations, but it considers clear from the *travaux préparatoires* of the European Patent Convention that algorithms are regarded as a pure mathematical-logical exercise and accordingly the abstract formulation of algorithms does not belong to a technical field.

[173] See however G. NOTO LA DIEGA, "Software Patents and the Internet of Things in Europe, the United States and India", *EIPR*, 2017, p. 173.

of this, it has been argued that securitization seems to have become the new paradigm of IPRs and public interest-oriented transparency function seems to have been marginalized [174]. The only way to recover from this trend may be to propose a balanced reading of trade secrets texts, such as the Trade Secrets Directive. As stated above, this legal tool is aimed at fostering innovation, but also circulation of information and this requires then a balanced approach as to the implementation of protection and to its limits[175]. In this perspective, it is pivotal to interpret its clauses in light of the proportionality principle and by taking into account all the views of the different interests stakeholders involved, such as investors and innovators, but also subjects, such as consumers, who have an interest in an increased circulation of the information[176].

Finally, trade secrets protection in the EU seems to serve well the purposes of the data economy in the IoT sector. In particular, it does not destabilize market operators and overall, it seems to respect fundamental rights. However, from a consumer's perspective, such a balanced reading may not be enough. Trade secrets need to be considered holistically and complemented by other legal instruments to take duly into account consumers interests. We argue that personal data protection laws can be successfully invoked by consumers who are negatively affected by IoT traders' data appropriation practices.

IV. Trade Secrets and Personal Data: Which Interfaces?

To demonstrate the thesis that consumers can invoke data protection to counter IoT companies' data appropriation practices, it is pivotal to critically analyse the relationship between trade secrets and personal data protection. Tensions over the control of IoT data can arise at the confluence of data protection laws and trade secrets. Nonetheless, there has been little effort to investigate the interplay between these two regimes.[177] Both personal data and trade secrets may consist of semantic information and this statement touches upon a crucial question, which is the reach of trade secrets protection in the case of personal data[178].

The Trade Secrets Directive declares a generic respect of the right to data protection and does not envisage a conflict with the GDPR.[179] This can be seen in Recital 34 of the Trade Secrets Directive, whereby the Directive "respects (…) the right to respect for private and family life (and) the right to protection of personal data" as enshrined in the

[174] G. SCHNEIDER, "European Intellectual Property and Data Protection in the Digital-Algorithmic Economy: A Role Reversal(?)", *JIPLP*, 2018, p. 229.
[175] The teleological interpretation of the text shared here is due to A. OTTOLIA, "Il D. Lgs n. 63/18", cit..
[176] Should we adopt a teleological criterion to interpret the Trade Secrets Directive and in particular Recital 16 and 21.
[177] J. DREXL, "Designing competitive markets", cit., 257; G. MALGIERI, "Trade Secrets v Personal Data: a possible solution for balancing rights", *International Data Privacy Law*, 2016/2, p. 102; G. SCHNEIDER, *op. cit.*, p. 229; G. NOTO LA DIEGA, "Against the dehumanisation of decision-making. Algorithmic decisions at the crossroads of intellectual property, data protection, and freedom of information", *JIPITEC*, 2018/1, p. 3.
[178] The analysis is found in G. SURBLYTĖ, *Data Mobility at the Intersection of Data, Trade Secret Protection and the Mobility of Employees in the Digital Economy*, *GRUR int*., 2016, p. 1121, in particular when a company uses social media accounts for the promotion of its business and claims trade secrets protection.
[179] The Trade Secrets Directive refers to the Data Protection Directive because it was adopted before the coming into effect of the GDPR. In the body of the text, however, we will replace the references to the Data Protection Directive with reference to the GDPR.

Charter of Fundamental Rights of the EU.[180] This is followed by the clarification that the GDPR governs the processing of personal data that takes place whilst taking steps to protect a trade secret and in proceedings on the unlawful acquisition, use or disclosure of trade secrets.[181] The conclusion is that the Trade Secrets Directive "should not affect the rights and obligations laid down in"[182] the GDPR. Considering the GDPR's philosophy of openness and control, this assumption that the two regimes converge is debatable. For example, an IoT company may seek its users' consent to collect their data and commercialise them, but it is unclear what happens if the consumers wants to access these data, especially once they have been aggregated with other secret information and they are now difficult to isolate. Regardless of the Directive's assumption that no conflicts will arise, trade secrets and personal data protection do and will indeed clash. Therefore, it is crucial to understand how to govern such conflict.

It should be noted that the aforementioned provisions are not binding as they are found in the Trade Secrets Directive's recitals. The only relevant binding provision is Article 9(4) whereby the processing of personal data in the course of legal proceedings relating to the unlawful acquisition, use or disclosure of a trade secret must comply with the GDPR. This is significant for two reasons. First, it shows a single-minded conception of the GDPR as a confidentiality centred law. Indeed, the legal proceedings this provision refers to are the proceedings for the "(p)reservation of confidentiality" and the national implementation measures confirm this by imposing obligations of confidentiality, but not an express duty to comply with the GDPR.[183] Second, the fact that this is the only binding provision that refers to data protection may be interpreted as meaning that the rest of the trade-secret-related processing, e.g. acquisition of the trade secret, must not necessarily comply with the GDPR.

Against this interpretation, and to show that trade secrets holders must always comply with the GDPR, arguments can be based on both the Trade Secrets Directive and the GDPR. Starting off with the former, we have seen in Section III that there are some exceptions that allow for competing interests to be balanced against – and even prevail on – the trade secret holder's interests. Of more direct relevance from this paper's perspective are the legitimate interest exception[184] and the freedom of information one.[185] Both can be relied on to claim that the unauthorised acquisition, use or disclosure of an IoT company's trade secrets that include the defendant's personal data are not unlawful either because data protection is a legitimate interest recognised by EU and national laws, or because the GDPR can be seen as an expression of the fundamental freedom to access information. This can be seen with particular clarity from the perspective of the rights to be informed,[186] of access[187] and not to be subject to an automated decision.[188]

[180] Charter of Fundamental Rights of the European Union, O.J. C 202, 7.6.2016, p. 389, arts 7 and 8.
[181] Trade Secrets Directive, recital 35.
[182] Trade Secrets Directive, recital 35.
[183] See Italy's Industrial Property Code, art 121-ter; France's Code of Commerce, art L 153-2; and the UK's Trade Secrets Regulations, reg 30.
[184] Trade Secrets Directive, art 5(d).
[185] Trade Secrets Directive, art 5(a).
[186] GDPR, arts 13-14.
[187] GDPR, art 15.
[188] GDPR, art 22.

Therefore, it would seem that, despite the Trade Secret Directive's assertion that there is no conflict between trade secrets and data protection, conflicts may occur and the trade secrets' exceptions should not be underestimated as a governance tool.

Once demonstrated that the GDPR applies to trade secrets, the extent to which it applies should be clarified in order to understand whether it can be invoked by an IoT user who is negatively affected by a trade secret.

Unlike the Trade Secrets Directive, the GDPR does not expressly regulate the interplay between the two instruments. The only visible interface is constituted by Recital 63, which states that the right of access "*should not adversely affect the rights or freedoms of others including trade secrets*"[189]. Thus, the GDPR recognises that trade secrets and data protection may conflict and that a balance should be struck between the right to maintain the secrecy of valuable commercial information and the right to access that information when it includes personal data. Concerns have been expressed that the trend to appropriate algorithms by means of trade secrets may render transparency unfeasible.[190] However, Recital 63 should not be interpreted as meaning that trade secrets in principle prevail on data protection. Such conclusion is based on three arguments.

First – and this is a key difference between the GDPR and the Data Protection Directive[191] – Recital 63 of the GDPR clarifies that the result of trade secrets considerations "*should not be a refusal to provide all information to the data subject"*. The Article 29 Working Party observed that the provision whereby trade secrets should not be adversely affected is to be interpreted narrowly; indeed, "controllers cannot rely on the protection of their trade secrets as an excuse to deny access or refuse to provide information to the data subject"[192]. The GDPR includes a best practice recommendation whereby organisations should be able to provide remote access to a secure self-service system which would provide the individual with direct access to his or her information.[193] The Information Commissioner's Office implies that such a system should not include trade secrets.[194] And indeed, allowing automated remote access would not be consistent with the reasonable steps that the holder has to take to keep the commercial information secret.[195] Therefore, the indication that the right of access should not adversely affect trade secrets should be interpreted as a right not to allow remote automated access to the personal data that the company holds. However, IoT companies, and all data controllers, must grant access on a case-by-case basis. Companies should distinguish the data whose disclosure would nullify the secrecy of the relevant commercial information and the data that can be disclosed without nullifying said secrecy. In allowing access to personal data covered by a trade secret, courts shall dictate measures that safeguard the commercial value of the trade secret, for instance by preventing its further disclosure.[196]

---

[189] GDPR, recital 63. See M. T. RIBEIRO ET AL., "Why Should I Trust You?: Explaining the Predictions of Any Classifier", in *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, New York City, ACM, 2016, p. 1135; A. B. TICKLE ET AL., "The Truth Will Come to Light: Directions and Challenges in Extracting the Knowledge Embedded within Trained Artificial Neural Networks", *IEEE Trans. Neural Netw*., 1998/6, p. 1057.

[190] This was an interpretation of recital 63 that was suggested, albeit in passing by G. SCHNEIDER, *op. cit*., 237.

[191] G. MALGIERI, "Trade secrets", cit., 103.

[192] ARTICLE 29 WORKING PARTY, "Guidelines on Automated individual decision-making", cit., p. 17

[193] GDPR, recital 63.

[194] INFORMATION COMMISSIONER'S OFFICE, *Guide, cit.*, p. 105.

[195] Trade Secret Directive, art 2(1)(c).

[196] G. NOTO LA DIEGA, *Against the dehumanisation*, cit., [87].

Second, in Recital 63 trade secrets are just an example of the importance to consider third parties' rights when exercising the right of access. That right should not adversely affect the "rights or freedoms of others, *including* trade secrets". This is crucial because under Article 15 of the GDPR, which deals with the right of access, rights and freedoms of others should not be adversely affected by the "right to obtain a copy"[197] of the data undergoing processing. This right to obtain a free-of-charge copy of one's personal data is only one of the powers that the right of access gives data subjects.[198] Under Article 15[199], the right of access means:

(i) A right to obtain confirmation as to whether one's personal data are processed;
(ii) That being the case, a right to access – and obtain a copy of – the data that are being processed; and
(iii) A right to obtain information about some key features of the processing. These include the purposes of the processing, their sources, and the existence of – and the logic involved in – automated decision-making.[200]

Therefore, IoT companies should not be allowed to invoke their trade secrets to deny a data subject's request to receive a copy of its data; they can only exclude data that cannot be isolated from the information covered by the trade secrets. Conversely, we argue that these companies, and more generally companies that hold trade secrets covering personal data, must:

(i) Release a copy of the rest of the data;
(ii) Confirm that data are being processed;
(iii) Grant access to key information, including the purposes of the processing e.g. the inclusion in information covered by trade secrets; finally, more importantly,
(iv) Grant access to all the data, including the data covered by trade secrets, although in 'view only' mode.

For example, if the data appropriated by an IoT company can play a role in the data subject's defence in legal proceedings – and such data cannot be isolated from the rest of the information covered by the trade secret – the company at the very least should allow the parties' representatives and the court to view the relevant data.

Third, alongside the right of access, the only data protection right on which trade secrets can, under certain circumstances, prevail is the right to portability, that is the right to receive one's personal data in a structured, commonly used and machine-readable format and to transmit it to another controller.[201] For example, in principle, users of Amazon's Echo who would like to switch to another smart home virtual assistant, for example Google Home, have an interest in transmitting the data that Echo has been collecting about them to Google. Thus, the new virtual assistant would learn more quickly

---

[197] GDPR, art 15(4), that refers back to art 15(3).
[198] INFORMATION COMMISSIONER'S OFFICE, *Guide*, cit., p. 102. Cf. M. DI MARTINO, "Personal Information Leakage by Abusing the GDPR 'Right of Access'", in *Proceedings of the Fifteenth Symposium on Usable Privacy and Security*, Berkeley, Usenix, 2019, p. 371.
[199] See, in particular, GDPR, art 15(1)(a), (g), (h), and 15(3)
[200] In particular on this topic see M. VEALE, L. EDWARDS, "Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling", *Computer Law & Security Review*, 2018/2, p. 398; I. MENDOZA, L. A. BYGRAVE, "The Right Not to Be Subject to Automated Decisions Based on Profiling", in T. E. SYNODINOU ET AL. (eds.), *EU Internet Law: Regulation and Enforcement*, Cham, Springer, 2017, p. 77; S. WACHTER ET AL., "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation" *IDPL*, 2017/2, p. 76.
[201] GDPR, art 20.

about the user's preferences and habits and would provide a more personalized service.[202] Under Amazon's Privacy Policy users can "ask for data portability (…) subject to applicable law".[203] The reference to the applicable law surely includes Article 20(4) of the GDPR whereby the right to data portability "shall not adversely affect the rights and freedoms of others". Although the Article 29 Working Party interprets this phrase as referring mainly to third parties' personal data protection,[204] it may as well be construed as including trade secrets. Consumers should not be advised to rely on the right to data portability to counter IoT companies' data appropriation practices. Indeed, unlike the right of access, the right to data portability is excluded as such if its exercise adversely affects trade secrets. Nonetheless, the result of trade secrets considerations "should not be the refusal to provide all information"[205]. Therefore, IoT companies should endeavor to isolate the requesting data subject's personal data and facilitate their portability.[206]

The rights to obtain a copy and to portability are the only data subject's rights that can be, to some extent, compressed if they adversely affect the rights and freedoms of others, including trade secrets. Therefore, relying on an *argumentum a contrario*, we claim that IoT companies cannot invoke their trade secrets to shield their data appropriation practices from the other data subjects rights. In principle, when it comes to the other data subject's rights and data controller's obligations, trade secrets will not be a valid legal basis for any exceptions or limitations.[207] This means that trade secrets will not limit the rights to be informed, to rectification, to erasure, to restrict processing, to object, and not to be subject to automated decision-making. Of these rights, those who can better empower consumers who are victims of IoT companies' data appropriation practices are the right to be informed and the right not to be subject to automated decisions.

The right to be informed is expression of the principle of transparency, that is a component of the first data protection principle under the GDPR (lawful, fair, and transparent processing). Transparency appears to be the opposite of secrecy, in that it creates an obligation to be clear, open and honest with users about how and why their personal data is processed.[208] Transparency is intrinsically linked to fairness and it applies to three central areas:

(i) The provision of the information about which data is processed and how;
(ii) The provision of information about data subject rights;
(iii)The way data controllers facilitate the exercise by data subjects of their rights.[209]

---

[202] See ARTICLE 29 WORKING PARTY, "Guidelines on the right to data portability" 2017/WP242 rev.01.
[203] Amazon's Privacy Policy, "What Choices do I Have?".
[204] ARTICLE 29 WORKING PARTY, "Guidelines on the right to data portability", cit., 12.
[205] Ibidem.
[206] Indeed, "(a) potential business risk cannot (…) serve as the basis for a refusal to answer the portability request and data controllers can transmit the personal data provided by data subjects in a form that does not release information covered by trade secrets or intellectual property rights" (ibidem).
[207] This is not to say that the exercise of the other rights will not be balanced against competing interests. A good example is the right to erasure that can be limited to the extent necessary to exercise freedom of expression and other listed legitimate interests. However, apart from access and portability, no other provision contains the generic proviso not to adversely affect the rights and freedoms of others, that is the prime entry point for trade secrets. On balancing the right to erasure against competing interests see J. AUSLOOS, *The Right to Erasure in EU Data Protection Law,* Oxford, Oxford University Press, 2020, part II.
[208] INFORMATION COMMISSIONER'S OFFICE, *Guide,* cit., p. 22.
[209] ARTICLE 29 WORKING PARTY, "Guidelines on transparency under Regulation 2016/679*",* 2018/WP260 rev.01, p. 4.

For the purposes of this paper, it is sufficient to focus on (i), as it is the most likely to apply to a scenario where an IoT company attempts to appropriate its users' personal data by means of a trade secret.

IoT companies who process personal data must inform consumers in a concise, transparent, intelligible, and easily accessible way.[210] The information – to be provided at the time when personal data is obtained[211] or within a month[212] – includes the purposes of the processing, the entities with whom the data is shared, the existence of the right to access the data, as well as the existence and the logic involved in automated decision making.[213] Users should be able to "*determine in advance what the scope and consequences of the processing"* entails and that they should not be taken by surprise at a later point about the ways in which their personal data have been used"[214]. Therefore, the IoT company should be very clear about the consequences that appropriating personal data, for example in the context of opaque algorithms, can have on the user.

There are limited exceptions to the obligation to inform and they apply only when personal data are obtained from sources other than the user (e.g. data brokers).[215] When this is the case, data controllers do not have to inform users if the latter already has the information; providing it would be impossible, require a disproportionate effort, or render impossible the achievement of the objectives of the processing; the processing is required by law; or an obligation of professional secrecy covers the data.[216] The reference to professional secrecy means that trade secrecy, as such, does not constitute an exception and in principle IoT companies that hold trade secret must fully comply with the obligations to inform. Conversely, said companies may try and argue that informing the user would make impossible the achievement of the objectives of the processing. This does not provide a blanket exemption to IoT companies holding trade secrets. They have to prove that the provision of information "would *nullify* the objectives of the processing"[217] The disclosure of the trade secret per se may nullify said objectives, the extraction of the personal data involved in that processing would not, or not necessarily. At any rate, IoT companies relying on this exception would still need to satisfy all the data protection principles,[218] including fairness and lawfulness.[219] This means that they "should only handle personal data in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them"[220]. If not properly informed, we do not see how IoT users would expect their traders to appropriate their data by means of trade secrets. Equally, there is little doubt that such appropriation may have unjustified adverse effects on them. This is well exemplified by Facebook's use of proprietary algorithms to manipulate its users' emotions.[221] Additionally, for processing to be lawful, the IoT

[210] GDPR, art 12.
[211] GDPR, art 13(1).
[212] GDPR, art 14(3)(a).
[213] GDPR, arts 13-14.
[214] ARTICLE 29 WORKING PARTY, *Guidelines on transparency*, cit., 7, italics added.
[215] C. J. HOOFNAGLE, "Big brother's little helpers: How ChoicePoint and other commercial data brokers collect and package your data for law enforcement" *NCJ Int'l L. & Com. Reg.*, 2003/29, p. 595.
[216] GDPR, art 14(5).
[217] ARTICLE 29 WORKING PARTY, *Guidelines on transparency*, cit., p. 31. Italics added.
[218] GDPR, art 5.
[219] ARTICLE 29 WORKING PARTY, *op. loc. ult. cit.*
[220] INFORMATION COMMISSIONER'S OFFICE, *Guide*, cit., p. 22.
[221] C. FLICK, "Informed consent and the Facebook emotional manipulation study" *Research Ethics*, 2016/1, p. 14.

company will have to prove that they rely on one of six legal bases, the main of which being consent and legitimate interest.[222]

Consent must be, amongst other things, informed, freely given, and easy to withdraw. This means that even IoT companies that attempt to rely on the aforementioned exception will have to inform users while collecting their consent. For the consent to be informed, the data subject should at least know,[223] the controller's identity, the processing's purposes, the type of data that will be collected, the existence of the right to withdraw, the use of automated decision-making systems, and the risks of international data transfers. IoT companies must be wary of the fact that they have to inform their users thoroughly if they want to benefit from a partial alleviation from the obligations to inform. Crucially, under no circumstances they will be able to hide the purpose for which they are appropriating their users' personal data. Moreover, consent can only be valid if freely given, which will not usually be the case when there is a power imbalance, and "if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences"[224] , which will rarely be the case in the IoT. IoT companies hold data power, that is multifaceted form of power arising from the control over data flows.[225] Thanks to this data power, IoT companies are free to impose their data practices – and the data subjects are forced to accept. In any event, consent can be withdrawn at any moment and in a way that is as easy as was giving consent.[226] IoT companies should, therefore, be aware of the fact that they should immediately stop the processing and erase the data should consent be withdrawn. This may affect the trade secrets that had incorporated the users' personal data. Such risk may induce IoT companies that hold trade secrets to rely on another legal basis for processing, namely legitimate interest.[227]

IoT companies may attempt and justify their data processing by claiming that it is necessary for the purposes of the legitimate interests pursued by them. The Court of Justice in *Rigas*[228] set forth a three-part test to assess whether legitimate interest can act as a valid legal basis. The first limb is the purpose test, which inquires whether there is a legitimate interest behind the processing. The second limb is necessity – is the processing necessary for that purpose? Finally, the balancing test, that is focused on ascertaining whether the individual's interests, rights, and freedoms override the company's legitimate interests. 'Purpose' is easily made out because even trivial corporate interests may qualify, as long as they are not vague or illegitimate (e.g. sending spam emails).[229] IoT companies may be able to prove that their business model is based on the appropriation of personal data. Necessary does not mean "absolutely essential, but it must be a targeted and proportionate way of achieving your purpose".[230] Again, depending on how important data appropriation

[222] GDPR, art 6.
[223] ARTICLE 29 WORKING PARTY, "Guidelines on consent under Regulation 2016/679" 2018/WP259 rev.01, p. 22.
[224] ARTICLE 29 WORKING PARTY, *op. ult. cit.*, p. 7.
[225] O. LYNSKEY, *op. loc. ult. cit.*
[226] GDPR, art 7(3).
[227] GDPR, art 6(1)(f).
[228] Judgment of 4 May 2017, C-13/16, Valsts Policijas Rigas Regiona Parvaldes Kartibas Policijas Parvalde v Rigas Pasvaldibas SIA Rigas Satiksme, EU:C:2017:336.
[229] INFORMATION COMMISSIONER'S OFFICE, "Legitimate interests*"* (*ICO*) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/#three_part_test> accessed 4 May 2020.
[230] Ibidem.

is to a business, IoT companies may meet the test. The real hurdle is the balancing test. Data controllers have to carry out a risk assessment and understand if the user's interests, rights, and freedoms prevail.[231] This includes the rights to privacy and data protection, but also other human rights enshrined in the Charter of Fundamental Rights of the EU and more general interests.[232] While privacy-intrusive practices cannot be justified by a company's legitimate interest, Recital 75 of the GDPR asks data controllers – and, ex post, courts – to consider whether the processing may lead to some physical, material or non-material damage. These include discrimination, financial loss, damage to the reputation, or "any other significant economic or social disadvantage"[233]. The appropriation of IoT data by means of trade secrets is likely to be privacy-intrusive and to disadvantage the user in manifold ways; therefore, IoT companies should not rely on their own legitimate interests and should fall back on consent.

It follows that, in most cases, IoT companies have to thoroughly inform users about their data appropriation practices. The principle of transparency, which underpins the obligations to inform, may act as a counterweight to trade secrecy. Being informed of data appropriation is the prerequisite for the consumers to act and attempt to stop it or minimise its risks. Consumers can rely on another right to actively defend themselves from IoT companies who weaponise their appropriated personal data, for example by using their algorithms to take automated decisions that can have profound consequences (e.g. automated screening of job applications).[234] The main tool that the GDPR makes available in these sort of scenarios is the right not to be subject to an automated decision.[235]

The right[236] not to be subject to an automated decision can be invoked if three requirements are made out: the individual is subject to a (i) decision, that is (ii) based solely on automated processing, and (iii) produces legal effects concerning the individual or similarly significantly affect them.[237] For example, Amazon should not be allowed to automatically exclude from its IoT platforms some users based on their ethnicity. Such automated systems should never be put in place if their decision can profoundly affect data subjects.[238]

The restriction on solely automated decision-making can be lifted on three grounds: contractual necessity, statutory authorisation, and explicit consent.[239] The restriction cannot be lifted if the controller processes special categories of data (e.g. health data), unless

---

[231] GDPR, art 6(1)(f).
[232] INFORMATION COMMISSIONER'S OFFICE, *op. loc. ult. cit.*
[233] GDPR, recital 75.
[234] T.C. SANDANAYAKE ET AL., "Automated CV Analyzing and Ranking Tool to Select Candidates for Job Positions", in *Proceedings of the 6th International Conference on Information Technology: IoT and Smart City*, New York City, ACM, 2018, p. 13.
[235] GDPR, art 22.
[236] It is controversial whether this is a right or a ban, though the second option seem to prevail. See ARTICLE 29 WORKING PARTY, "Guidelines on Automated individual decision-making", cit., p. 12; G. NOTO LA DIEGA, "Against the dehumanisation", cit., [47].
[237] GDPR, art 22(1). These concepts are problematic but they are of little relevance from this paper's perspective and therefore they will not be analysed. For more information on this see ARTICLE 29 WORKING PARTY, "Guidelines on Automated individual decision-making", cit., p. 20.
[238] Automated IoT decisions can also have positive effects. See S. ROY, R. BOSE, D. SARDDAR, "A Fog-Based DSS Model for Driving Rule Violation Monitoring. Framework on the Internet of Things" *International Journal of Advanced Science and Technology*, 2015/82, p. 23.
[239] GDPR, art 22(2).

special circumstances apply e.g. the processing is necessary for substantial public interest reasons.[240]

Contractual necessity, statutory authorisation, and explicit consent do not provide a carte blanche; an IoT company that would rely on them would have to implement suitable safeguards for the data subject's rights, freedoms, and legitimate interests. They include, at least, the right to obtain human intervention on the part of the controller, to express their point of view and to contest the decision.[241] It is debated whether one of the safeguards is the right to obtain an explanation of the decision. On the one hand, it can be argued that since such right is only referred to in a non-binding recital, but Article 22 did not refer to it, there would be no right to an explanation.[242] On the other hand, based on a more systematic interpretation that takes into account the principle of transparency and the obligations to inform, it can be argued that a right to an explanation exists.[243] And indeed, the fact that the right to an explanation is referred to in a non-binding recital should not be overstated. The pivotal role of recitals in interpreting the provisions of an EU act has been expressly recognised.[244] The reference to the right of explanation in the recital shall be, therefore, used to properly construe Article 22 to reflect the context of the provision and the overall purpose of the GDPR, that is increasing the protection of the data subjects' rights. Hence, even though applying the literal rule, Article 22 would not contain a right to explanation, a purposive approach and a correct valorisation of the role of recitals make it clear that data subjects are entitled to such a right. In any event, should one be of the view that the right to an explanation does not exist, the right to inform expressly includes the obligation to inform about the existence of automated decision-making and to provide meaningful information about the "logic involved, as well as the significance and the envisaged consequences of such processing for the data subject"[245]. This means that IoT companies that hold trade secrets should not use algorithmic or otherwise automated systems to take decision that can negatively affect the user. If they do so, for example because the user gave them explicit consent, they still need to put in place some safeguards that at the very least include an obligation to explain the logic involved in the algorithmic decision and the right to a human being reviewing the decision. IoT companies will not be able to oppose their trade secrets as a valid reason not to provide meaningful information about their algorithmic decisions. Thus, there is a major difference with the US approach as epitomised in *State v Loomis*,[246] when Mr Loomis has been considered dangerous by an algorithmic system and had not been able to contest the decision because the system was proprietary. In the EU, stronger protection to personal data and right to a fair trial would not allow such an outcome.[247]

---

[240] GDPR, arts 22(4) and 9.
[241] GDPR, art 22(3).
[242] WACHTER ET AL., "Why a Right to Explanation", cit., p. 76.
[243] G. MALGIERI, G. COMANDÉ, "Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation" *IDPL*, 2017/4, p. 243. On the optimistic front, see also J. POWLES - H. HODSON, "Google DeepMind and healthcare in an age of algorithms", *Health Technol.* 2017, p. 351; G. NOTO LA DIEGA, *Against the dehumanisation,* cit., p. 72.
[244] R. BARATTA, "Complexity of EU law in the domestic implementing process", *19th Quality of legislation seminar "EU legislative drafting: Views from those applying EU law in the Member States*, 2014, p. 4.
[245] GDPR, arts 13(2)(f) and 14(2)(g).
[246] 881 N.W.2d 749 (Wis. 2016)
[247] Cf. H., W. LIU, C.-F. LIN, Y.-J. CHEN, "Beyond State v Loomis : artificial intelligence, government algorithmization and accountability", *International Journal of Law & Information Technology* 2019, p. 122.

This should be caveated by the observation that the GDPR does allow Member States to introduce restrictions to all data protection rights – not just to the rights of access and of portability – "when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard… the protection of the data subject or the rights and freedoms of others"[248]. Of the selected jurisdictions, only France took advantage of this option.[249] Indeed, the *Loi informatique et libertés* provides that when an automated decision is justified by contractual necessity or explicit consent, the data controller, alongside ensuring human intervention, the right to express one's point of view, and to contest the decision, must communicate the rules that define the processing and the main characteristics of its implementation "*à l'exception des secrets protégés par la loi*".[250] It is fair to infer that these secrets protected by the law encompass trade secrets. This does not mean, however, that consumers who are based in France cannot rely on Article 22 of the GDPR to counter IoT data appropriation. It merely means that, in informing about the automated system, the controller does not have to disclose trade secrets. Nonetheless, France-based IoT companies will have to:

(i) Abide by the general ban on solely automated decisions, unless they have secured user consent or demonstrated contractual necessity;
(ii) Respect the other GDPR rights, including the right to be informed about the logic involved in the automated decision ; and
(iii) Endeavour to isolate consumers' personal data from the rest of the information that is covered by trade secrets and inform consumers accordingly.

V. Conclusion

In an IoT world where personal data are appropriated by private companies by multiple means, including trade secrets, there is a palpable tension between data protection laws and trade secrecy.

[248] GDPR, art 23(1)(i).

[249] As a general statement, regardless of this transposition, this principle may be recognised in other jurisdictions too; in fact, it is reasonable to affirm that the legal order aims at balancing different and sometimes conflicting interests via the principle of proportionality. The UK introduced some exception in the part of the Data Protection Act 2018 that implements the Law Enforcement Directive and therefore only applies to "processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties" (Law Enforcement Directive, art 1(1)). In particular, when processing data for law enforcement purposes, the data controller "may restrict, wholly or partly, the provision of information to the data subject (…) *to the extent that and for so long as* the restriction is, having regard to the fundamental rights and legitimate interests of the data subject, a *necessary and proportionate* measure to (…) protect the rights and freedoms of others" (Data Protection Act 2018, s 44(4)(e)). Similar provisions apply to the right of access (s. 45(4)(e)), the obligation to inform about the refusal to rectify, erasure or restrict processing (s 48(3)(e)), and the obligation to communicate a data breach to the data subject (s 68(7)(e)). These provisions regard law enforcement and are unlikely to apply to IoT processing; therefore, they have been left out of the scope of this paper. Similar considerations apply to the French provisions whereby – when data is processed for law enforcement purposes – the communication of the breach to the data subject and the latter's rights can be restricted if necessary and proportionate to "*(p)rotéger les droits et libertés d'autrui*" (*Loi informatique et libertés*, arts 102(3) and 107(1)(5)). Similarly, in Italy, see Decreto Legislativo 18 May 2018 n. 51 (Law Enforcement Directive Implementing Decree), art 14(2)(d).

[250] *Loi* n° 78-17, art 47(1)

There is not sufficient evidence to conclude that, in principle, one regime will always prevail on the other. This will have to be decided on a case-by-case basis.[251] However, we argue that some of the trade secrets' limits and data protection considerations can be invoked to counter the opaque data appropriation practices of IoT companies such as Amazon and Google.

The Trade Secrets Directive provide some exceptions that can be invoked to justify the unauthorised acquisition, use, and disclosure of trade secrets. Data protection is a legitimate interest protected by both EU and national laws. Accordingly, data subject whose data have been appropriated may claim control over their data, despite their integration in trade secrets held by IoT companies, inasmuch as the data subject's activity is necessary to protect their legitimate interest – and fundamental right – to personal data protection. Data subjects may also rely on the trade secret exception for freedom of information purposes because the GDPR is an expression of such freedom. On the other hand, the GDPR recognises that the right of access and to data portability should not adversely affect trade secrets. The key point is that trade secrets considerations cannot justify blanket refusals to comply with data subjects' requests. IoT companies that hold trade secrets cannot deny access to data subjects' personal data, the only exemption is from the right to provide a copy of the data, which is only one of the components of the right of access. Consumers can still invoke the other components of the right of access, namely the right to obtain confirmation as to whether one's personal data is processed; the right to obtain information about some key features of the processing; and the right to access the data that is being processed, albeit in 'view only' mode.

Trade secrets considerations can justify only limited restrictions to access and portability, but the other individual rights, principles and obligations still apply and can be used to counter IoT companies' data appropriation. Amongst these rights, it seems likely that an important role will be played by the right to be informed and the right not to be subject to automated decisions. In granting data subjects' requests, IoT companies have to endeavor to isolate consumers' personal data from the rest of the information that is covered by trade secrets.

In conclusion, we hope that a holistic and perhaps non-conventional approach to consumer protection, that integrates trade secrets' exceptions and data protection rights, can empower IoT consumers by opening the black box created by opaque data appropriation practices.

[251] G. MALGIERI, "Trade secrets*",* cit, 104, convincingly concluded that "it is incorrect to say that data protection law accepts a prevalence of trade secrets rights, and trade secret law accepts a prevalence of data protection rights: they just affirm a 'non-prevalence' of their rules. Therefore, the only possible conclusion is that no discipline prevails a priori on the other one".